

CLARENDON COLLEGE

BOARD OF REGENTS

March 27, 2025

Posted Agenda
&
Certification of Notice Posting

**PUBLIC NOTICE OF MEETING
CLARENDON COLLEGE BOARD OF REGENTS
AGENDA FOR REGULAR MEETING
BAIRFIELD ACTIVITY CENTER- VIP ROOM
CLARENDON COLLEGE – CLARENDON, TEXAS
THURSDAY, March 27, 2025**

POSTED
AT 3:00 O'CLOCK P M

MAR 24 2025

CLERK COUNTY COURT, DONLEY COUNTY, TEXAS

BY Mindy Steel Deputy

In compliance with the Open Meetings Act, Texas Government Code, Section 551.041, notice is hereby given that a regular meeting of the Clarendon College Board of Regents will be held on Thursday, March 27, 2025 at 6:00 PM at the Bairfield Activity Center VIP Room on the Clarendon Campus of Clarendon College, Clarendon, Texas. The subjects to be discussed, considered, or upon which any formal action may be taken during the regular meeting are as follows:

1. **CALL TO ORDER**
 - A. WELCOME
 - B. INVOCATION
 - C. REGENTS PRESENT/ABSENT
 - D. COLLEGE OFFICIALS PRESENT
2. **CERTIFICATION OF POSTING NOTICE OF MEETING**
3. **PUBLIC COMMENTS**
(PLEASE COMPLETE A REQUEST CARD PRIOR TO THE START OF THE MEETING. THE BOARD CHAIRPERSON MAY LIMIT THE TIME OF APPEARANCE BEFORE THE BOARD TO THREE MINUTES.)
4. **CONSIDERATION AND POSSIBLE ACTION ON MINUTES**
 - A. February 27, 2025 Regular Meeting
5. **CONSIDERATION AND POSSIBLE ACTION FINANCIAL REPORTS**
 - A. February 2025 Financials
 - BANK TO LEDGER TRANSACTIONS REFLECTED AND ACCOUNTS RECONCILED
 1. RECONCILIATIONS February 28, 2025
 - BUDGET TO ACTUAL ALL ACCOUNTS FY2025 TO February 28, 2025
 - VARIANCE ANALYSIS FOR THE MONTH OF February 2025
 - LISTING OF CHECKS OF OPERATION FOR MONTH OF February 2025
 - INVESTMENT REPORT- EDWARD JONES FOR THE MONTH OF February 2025
 - TAX REPORTS FOR DONLEY, CHILDRESS AND GRAY COUNTIES
6. **CONSIDERATION AND POSSIBLE ACTION ON 2nd QUARTER FY 2025 QUARTERLY REPORT**
7. **CONSIDERATION AND POSSIBLE ACTION ON CHANGES TO ROOM, BOARD AND COURSE FEES**
8. **CONSIDERATION AND POSSIBLE ACTION ON STRICKLAND FARM**
9. **CONSIDERATION AND POSSIBLE ACTION ON CHANGES IN TUITION AND MANDATORY FEES FOR 2025-2026 ACADEMIC SCHOOL YEAR**

*If during the course of the meeting any discussion of any items on the agenda or any other permitted matter(s) should be held in closed meeting, the Board will convene in closed meeting in accordance with the applicable section of the Texas Government Code, Title 5, Chapter 551.

10. CONSIDERATION AND POSSIBLE ACTION ON RESOLUTION OF SUPPORT FOR CONTINUED INVESTMENT IN THE DYNAMIC COMMUNITY COLLEGE FUNDING MODEL
11. CONSIDERATION AND POSSIBLE ACTION ON IT POLICY UPDATES
12. RATIFY NEW HIRES/RESIGNATIONS/APPOINTMENTS/REASSIGNMENTS & OTHER PERSONNEL MATTERS
 - A. NEW HIRES
 - Lexie Blackburn- Administrative Assistant to VP of Academic Affairs- Clarendon Campus, 4/1/2025
 - B. RESIGNATIONS
 - Morgan De La Cruz-Dual Credit Cosmetology- Pampa Center, eff. 5/16/2025
13. CLOSED SESSION* SECTION 551.074 (a)(1) - PERSONNEL MATTERS
14. CONSIDERATION AND POSSIBLE ACTION ON PERSONNEL MATTERS DISCUSSED IN CLOSED SESSION
15. REPORTS-NON-ACTION ITEMS
 - A. Faculty Senate Representative
 - Faculty Senate Meeting Minutes
 - B. Registrar
 - C. Vice President of Academic Affairs
 - SACSCOC Update
 - D. President's Report
 - BOR Self-Evaluations & Evaluation of President Forms
 - Commencement 5/9 10am; 1pm (RFO); 4pm; 7pm; Nursing Commencement 5/16 6pm
16. ADJOURNMENT

Texas D. "Tex" Buckhaults
President

*If during the course of the meeting any discussion of any items on the agenda or any other permitted matter(s) should be held in closed meeting, the Board will convene in closed meeting in accordance with the applicable section of the Texas Government Code, Title 5, Chapter 551.

Certification of Notice of Posting of Clarendon College Board of Regents Meeting

Type of Meeting: Regular Board of Regents Meeting 3/27/2025

Posted at the Donley County Annex (email, fax & posted to board) on 3/24/25 at 3:00pm (date & time)

by Cindy Upton (name)

Posted at the CC administration building on 3/24/25 at 3:20pm (date & time)

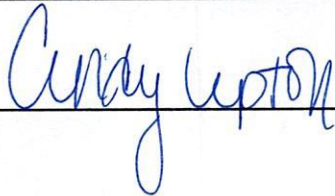
by Cindy Upton (name).

Posted on the CC Website on 3/24/25 at 3:30pm (date & time) by

Cindy Upton (name).



President



Assistant to the President

Minutes

CLARENDON COLLEGE BOARD OF REGENTS

MINUTES OF REGULAR MEETING THURSDAY, February 27, 2025

The Board of Regents of Clarendon College met in regular session on Thursday, February 27, 2025 at 6:00 p.m. in the VIP room of the Bairfield Activity Center of Clarendon College, Clarendon, Texas.

Board Vice Chairman, Lon Adams, called the meeting to order at 6:00 p.m.

AGENDA ITEM #1: The invocation was given by Regent, Clay Montgomery

Regents Present: Vice Chairman Lon Adams; and Members: Dr. Guy Ellis, Chris Matthews Jay Anders, Shaun O'Keefe and Clay Montgomery..

Regents Absent: : Chairman, Jim Shelton, Carey Wann and Secretary Janice Knorpp

College Officials Present: Tex Buckhaults, President; Michael Metcalf, Comptroller; Will Thompson, VP of IT; Cindy Upton, Assistant to the President and Brad Vanden Boogaard, Vice President of Academic Affairs. .

Others Present: Dr. Lauraine Paul, public comment.

AGENDA ITEM #2: CERTIFICATION OF POSTING NOTICE OF MEETING:

Motion by Shaun O'Keefe with a second by Chris Matthews to approve the Certification of Notice of posting of Board of Regents regular meeting for February 27, 2025. (copy attached to minutes)

Vote For: (6) Vote Against (0) Abstain (0)

AGENDA ITEM #3: PUBLIC COMMENT: Dr. Lauraine Paul spoke on behalf of her son, Tyler Paul in regards to credentials. (Please see attached public comment form).

AGENDA ITEM #4: APPROVAL OF MINUTES:

Motion by Chris Matthews with a second by Shaun O'Keefe that minutes of the regular meeting of January 23, 2025 be approved with corrections noted as regents present/absent at 1/23/2025 meeting to reflect that regent Carey Wann was NOT in attendance instead of being in attendance and all votes on agenda items requiring a vote be changed from 7-0-0 to 6-0-0 to reflect the correct number of regents voting on all items requiring a vote. (Please see attached corrected minutes). .

Vote For: (6) Vote Against (0) Abstain (0)

AGENDA ITEM #5: APPROVAL OF FINANCIAL REPORTS:

Motion by Clay Montgomery with a second by Shaun O'Keefe that financial statements, reports and expenses for the month of January 2025 be approved as presented.

Vote For: (6) Vote Against: (0) Abstain: (0)

AGENDA ITEM #6: ANNUAL REVIEW AND POSSIBLE ACTION ON APR RESOLUTION:

Motion by Shaun O'Keefe with a second by Shaun O'Keefe that financial statements, reports and expenses for the month of January 2025 be approved as presented.

Vote For: (6) Vote Against: (0) Abstain: (0)

AGENDA ITEM #7: CONSIDERATION AND POSSIBLE ACTION ON NEW IT CYBERSECURITY USER ACCOUNT PASSWORD POLICY:

Motion by Chris Matthews with a second by Shaun O'Keefe to approve the new IT Cybersecurity User Accounts Password Policy as presented.

Vote For: (6) Vote Against: (0) Abstain: (0)

AGENDA ITEM #8: CONSIDERATION AND POSSIBLE ACTION TO RATIFY NEW HIRES/RESIGNATIONS/APPOINTMENTS/REASSIGNMENTS & OTHER PERSONNEL MATTERS:

Motion by Dr. Guy Ellis with a second by Shaun O'Keefe to **RATIFY NEW HIRES/RESIGNATIONS/REASSIGNMENTS** as presented.

Vote For: (6) Vote Against (0) Abstain: (0)

AGENDA ITEM #9: REPORTS- NON-ACTION ITEMS:

This report is informational only and requires no action by the Board.

- A. Faculty Senate Representative
 - i. Faculty Senate Minutes
- B. Vice President of Academic Affairs
 - i. SACSCOC Update
- C. President's Report-
 - i. TACC- Preliminary Enrollment Report

AGENDA ITEM #10: ADJOURNMENT:

Lon Adams, Vice-Chairman of the Board announced, "If there is no objection, we will now adjourn the meeting. Hearing no objection, this meeting is now adjourned at 6:33pm. RONR (12 ed.) 21:15

Jim Shelton, Chair

Janice Knorpp, Secretary

Certification of Notice of Posting of Clarendon College Board of Regents Meeting

Type of Meeting: Regular Board of Regents Meeting 02/27/2025

Posted at the Donley County Annex (email, fax & posted to board) on 2/24/25 at 1:30pm (date & time)

by Cindy Upton (name)

Posted at the CC administration building on 2/24/25 at 2:00pm (date & time)

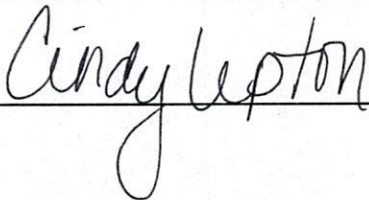
by Cindy Upton (name).

Posted on the CC Website on 2/24/25 at 2:05pm (date & time) by

Cindy Upton (name).



President

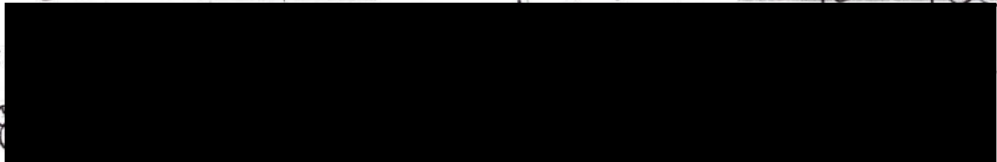


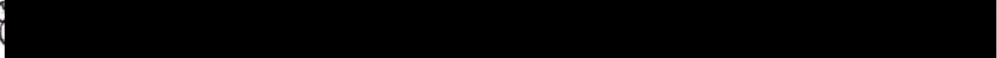
Assistant to the President

PUBLIC COMMENT FORM

Please print the following information:

Name: Laura Paul intyler Paul's place Today's Date: 2/27/25

Address: 

Phone: 

Organization Represented (if any): - Tyler Paul

Non-Speaker ☐ Speaker ☒

Agenda Item Number or Subject to be addressed: Credentials

Select applicable position on item: Support Oppose Neutral

Instructions & Rules of Procedure

1. This form must be submitted prior to commencement of the meeting.
2. This form must be completed and submitted for all citizens who wish to address the Board of Regents or register a formal position on an item being considered by the Board.
3. Please remember to stand up when you are recognized by the Board Chairman and state your name and address on behalf of an organization or other group, identify the group represented.
4. Speakers' time may not be pooled and given to other speakers.
5. All presentations by citizens are limited to no more than 5 minutes.
6. Board Chairman reserves the right to limit the number of citizens who may present on a particular agenda item if necessary to expedite the meeting in an efficient manner.
7. If you have written remarks or printed material you wish to present to the Board of Regents, please furnish it to the Assistant to the President for inclusion in the file for the agenda item.
8. Speakers should address all remarks to the Board of Regents as a whole, not to individual members.
9. All persons who complete this form, whether or not allowed to speak, may submit written comments or exhibits to the Board of Regents for inclusion in the file for the agenda item.
10. No shouting or cursing is allowed at Board of Regents meetings. Purposefully disrupting a public meeting is a violation of state law, and may result in the offending party being made to leave the meeting, and can lead to criminal charges.

PLEASE RETURN THIS REQUEST TO THE ASSISTANT TO THE PRESIDENT

CLARENDON COLLEGE BOARD OF REGENTS

MINUTES OF REGULAR MEETING THURSDAY, January 23, 2025

The Board of Regents of Clarendon College met in regular session on Thursday, January 23, 2025 at 6:00 p.m. in the VIP room of the Bairfield Activity Center of Clarendon College, Clarendon, Texas.

Board Chairman, Jim Shelton, called the meeting to order at 6:00 p.m.

AGENDA ITEM #1: The invocation was given by Regent, Dr. Guy Ellis.

Regents Present: Chairman, Jim Shelton; Vice Chairman Lon Adams; Secretary Janice Knorpp and Members: Dr. Guy Ellis, Jay Anders, and Clay Montgomery..

Regents Absent: Chris Matthews, CareyWann and Shaun O'Keefe

College Officials Present: Tex Buckhaults, President; Michael Metcalf, Comptroller; Will Thompson, VP of IT; Julie Morrow, Admin Assistant to VPAA.

Others Present: Chris Wilson and Sharlene Bordonero- Clarendon Chamber of Commerce Representatives.

AGENDA ITEM #2: CERTIFICATION OF POSTING NOTICE OF MEETING:

Motion by Jim Shelton with a second by Lon Adams to approve the Certification of Notice of posting of Board of Regents regular meeting for January 23, 2025. (copy attached to minutes)

Vote For: (6) Vote Against (0) Abstain (0)

AGENDA ITEM #3: PUBLIC COMMENT: None

AGENDA ITEM #4: APPROVAL OF MINUTES:

Motion by Jay Anders with a second by Janice Knorpp that minutes of the regular meeting of November 21, 2024 be approved as presented.

Vote For: (6) Vote Against (0) Abstain (0)

AGENDA ITEM #5: APPROVAL OF FINANCIAL REPORTS:

Motion by Janice Knorpp with a second by Clay Montgomery that financial statements, reports and expenses for the month of November 2024 be approved as presented with the exception of the bank reconciliations.

Vote For: (6) Vote Against: (0) Abstain: (0)

Motion by Clay Montgomery with a second by Dr. Guy Ellis that financial statements, reports and expenses for the month of December 2024 be approved as presented with the exception of the bank reconciliations.

Vote For: (6) Vote Against: (0) Abstain: (0)

AGENDA ITEM #6: CONSIDERATION AND POSSIBLE ACTION ON 1st QUARTER FY 2025 QUARTERLY REPORT:

Motion by Clay Montgomery with a second by Lon Adams to approve the 1st Quarter FY 2025 Quarterly Report as presented.

Vote For: (6) Vote Against (0) Abstain: (0)

AGENDA ITEM #7: ANNUAL REVIEW AND POSSIBLE ACTION ON CLARENDON CHAMBER OF COMMERCE REQUEST TO SERVE ALCOHOL AT BANQUET BEING HELD ON CLARENDON COLLEGE PROPERTY:

Motion by Janice Knorpp with a second by Dr. Guy Ellis to approve the chamber of commerce's request to serve alcohol during the first hour of the event and IDs will be checked.

Vote For: (6) Vote Against (0) Abstain: (0)

AGENDA ITEM #8: CONSIDERATION AND POSSIBLE ACTION ON STRICKLAND ESTATE: No Action Taken

AGENDA ITEM #9: CONSIDERATION AND POSSIBLE ACTION ON PURCHAS COOPERATIVE REBATE (ITEM TABLED AT OCTOBER 2024 REGULAR BOR MEETING: No Action Taken

AGENDA ITEM #10: CONSIDERATION AND POSSIBLE ACTION ON POLICY GK LOCAL:

Motion by Clay Montgomery with a second by Janice Knorpp to approve the new GK Local policy for creditors.

Vote For: (6) Vote Against (0) Abstain: (0)

AGENDA ITEM #11: CONSIDERATION AND POSSIBLE ACTION ON REGENTS TRAINING DOCUMENTATION: No Action Taken

AGENDA ITEM #12: CONSIDERATION AND POSSIBLE ACTION TO RATIFY NEW HIRES/RESIGNATIONS/APPOINTMENTS/REASSIGNMENTS & OTHER PERSONNEL MATTERS:

Motion by Janice Knorpp with a second by Lon Adams to **RATIFY NEW HIRES/RESIGNATIONS/REASSIGNMENT** as presented.

Vote For: (6) Vote Against (0) Abstain: (0)

AGENDA ITEM #13: REPORTS- NON-ACTION ITEMS:

This report is informational only and requires no action by the Board.

- A. Faculty Senate Representative
 - i. Faculty Senate Minutes
- B. President's Report-
 - i. Fall 2024 Athletic Director's Honor Roll

AGENDA ITEM #14: ADJOURNMENT:

Mr. Shelton, Chairman of the Board announced, "If there is no objection, we will now adjourn the meeting. Hearing no objection, this meeting is now adjourned at 6:54pm. RONR (12 ed.) 21:15

Jim Shelton, Chair

Janice Knorpp, Secretary

Financial Reports

Clarendon College
Bank Account Balances
As of February 28, 2025

Bank Account	Yield	Balance	
Operating	1.5000%	502,604.80	
Operating - PAL	4.0000%	3,013,019.01	^
Operating - Edward Jones	4.3000%	2,874,994.87	**
Operating - Texas Class	4.5786%	1,765,487.52	***
Capital Reserve	1.5000%	75,086.38	*
Capital Reserve - PAL	4.0000%	771,119.96	*/^
Agency Funds	1.5000%	75,086.34	*
Agency Funds - PAL	4.0000%	232,228.08	*/^
Agency Funds - Edward Jones	4.3000%	246,649.53	*/**
Childress - First United Bank	0.6000%	6,915.13	
Construction - Clarendon	1.5000%	5,005.77	*
Construction - Clarendon PAL	4.0000%	70,485.61	*/^
Construction - Pampa	1.5000%	5,761.64	*
Disbursement	0.0000%	3,525.80	
Equine	1.5000%	1,135.36	*
Interest & Sinking	1.5000%	1,466.80	*
Pampa - First Bank & Trust	1.9800%	9,502.31	
Payroll	1.5000%	21,346.87	
Title IV	0.0000%	10,000.00	*
Transportation	1.5000%	75,086.32	*
Transportation - PAL	4.0000%	258,777.58	*/^
Total		<u>10,025,285.68</u>	
* Restricted Funds		1,827,889.37	
Unrestricted Funds		<u>8,197,396.31</u>	
** Money held at Edward Jones		3,121,644.40	
*** Money held at Texas Class		1,765,487.52	
^ Herring Bank Sweep Account		4,345,630.24	
Money at Banks		<u>792,523.52</u>	

	2025 Budget	2025 Actual	Balance	% of Budget Expense	2024 Actual
<u>Educational and General Budget</u>					
<u>Revenue:</u>					
Tuition	2,227,500.00	2,069,591.57	157,908.43	92.91%	1,847,390.90
Student Fees	2,484,887.48	1,945,984.10	538,903.38	78.31%	2,055,869.20
Exemptions and Waivers	(167,000.00)	(111,204.79)	(55,795.21)	66.59%	(93,167.00)
State Appropriations	7,255,772.00	5,329,031.12	1,926,740.88	73.45%	4,552,108.86
Ad Valorem Taxes	1,920,000.00	1,728,625.82	191,374.18	90.03%	1,889,661.74
Miscellaneous Income	201,580.00	180,389.24	21,190.76	89.49%	385,872.82
Revenue - Education and General	13,922,739.48	11,142,417.06	2,780,322.42	80.03%	10,637,736.52
<u>Expense:</u>					
Business Administration-Clarendon	16,325.00	7,732.90	8,592.10	47.37%	3,298.86
Business Administration - Pampa	78,981.95	45,924.99	33,056.96	58.15%	33,246.52
Computer Science-Clarendon	0.00	0.00	0.00	0.00%	1,826.10
Developmental Studies-Clarendon	59,584.07	18,543.20	41,040.87	31.12%	6,631.37
Developmental Studies - Pampa	47,877.73	16,676.63	31,201.10	34.83%	0.00
Industrial Maintenance	5,700.00	4,750.19	949.81	83.34%	39,304.41
CDL - Pampa	233,787.35	110,116.60	123,670.75	47.10%	116,017.35
Mathematics-Clarendon	96,946.53	61,271.75	35,674.78	63.20%	47,626.18
Mathematics-Pampa	66,881.93	36,140.22	30,741.71	54.04%	27,952.59
Art - Clarendon	21,665.70	9,483.84	12,181.86	43.77%	8,306.35
Music	15,380.40	11,591.60	3,788.80	75.37%	433.07
History and Government-Clarendon	197,095.15	104,751.43	92,343.72	53.15%	82,148.96
History and Government - Pampa	73,248.31	43,734.61	29,513.70	59.71%	31,789.01
Languages and Literature-Clarendon	167,596.03	79,209.57	88,386.46	47.26%	90,062.26
Languages & Literature - Pampa	33,898.63	40,949.84	(7,051.21)	120.80%	28,642.16
Psychology & Sociology	116,484.39	62,236.28	54,248.11	53.43%	60,179.21
Speech Communications-Clarendon	79,246.52	48,042.38	31,204.14	60.62%	41,483.59
Criminal Justice-Clarendon	41,696.42	17,345.66	24,350.76	41.60%	25,530.44
Cosmetology Pampa	137,580.67	81,354.02	56,226.65	59.13%	67,959.35
Cosmetology Childress	139,309.48	60,579.36	78,730.12	43.49%	44,391.78
Cosmetology Amarillo	350,390.64	222,090.08	128,300.56	63.38%	167,005.89
Cosmetology Canyon	100,536.32	43,584.16	56,952.16	43.35%	71,225.27
Agriculture-Clarendon	102,937.34	55,953.34	46,984.00	54.36%	43,417.60
Welding-Clarendon	87,144.44	27,936.27	59,208.17	32.06%	21,357.34
Welding-Pampa	74,058.80	57,023.95	17,034.85	77.00%	13,814.77
Ranch & Feedlot Operations-Clarendon	177,216.18	89,313.10	87,903.08	50.40%	76,576.09
Health & Physical Education-Clarendon	91,759.50	70,509.76	21,249.74	76.84%	49,711.18
Science/Biology-Clarendon	108,577.64	75,022.67	33,554.97	69.10%	58,238.00
Science/Biology-Pampa	80,182.59	35,296.06	44,886.53	44.02%	28,929.18
Science/Biology-Childress	10,659.98	628.45	10,031.53	5.90%	2,232.59
Science/Chemistry-Clarendon	76,731.59	32,646.66	44,084.93	42.55%	28,145.67
Vocational Nursing - Pampa	258,137.80	145,976.62	112,161.18	56.55%	96,776.46
Vocational Nursing - Childress	377,337.36	140,820.56	236,516.80	37.32%	93,803.35
Registered Nurse - Pampa	256,679.59	93,775.53	162,904.06	36.53%	55,980.81
Registered Nurse - Childress	140,833.95	77,910.77	62,923.18	55.32%	53,712.52
Simulation Lab	79,488.82	39,596.42	39,892.40	49.81%	31,444.84
Cont Ed / Adult Ed - Pampa	9,558.50	501.26	9,057.24	5.24%	1,407.21
Corr Ed / Adult Ed - Pampa	150,526.37	56,320.52	94,205.85	37.42%	46,039.99
Instruction - General	161,121.75	44,832.75	116,289.00	27.83%	35,297.63

CLARENDON COLLEGE
BUDGET
For the Six Months Ending Friday, February 28, 2025

draft for discussion
ended 2/28/2025
printed 3/25/2025

	2025 Budget	2025 Actual	Balance	% of Budget Expense	2024 Actual
Honors College	0.00	0.00	0.00	0.00%	228.00
Instructional Administration-Clarendon	183,319.12	93,143.66	90,175.46	50.81%	77,322.12
Instructional Administration-Pampa	143,570.85	74,978.42	68,592.43	52.22%	74,240.45
Instructional Administration-Childress	109,440.30	143.17	109,297.13	0.13%	30,353.42
Library-Clarendon	105,430.27	59,820.60	45,609.67	56.74%	51,255.60
Library-Pampa	21,947.20	9,810.87	12,136.33	44.70%	6,121.05
Library-Childress	0.00	0.00	0.00	0.00%	5,707.11
Student Services-Clarendon	319,062.08	133,620.24	185,441.84	41.88%	86,038.82
Recruiting-Clarendon	98,592.94	8,384.90	90,208.04	8.50%	8,603.93
Recruiting - Pampa	6,500.00	0.00	6,500.00	0.00%	0.00
Associate Dean of Enrollment Services	118,173.42	72,670.17	45,503.25	61.49%	52,976.06
Associate Dean of CTE	19,358.93	8.10	19,350.83	0.04%	9.52
Testing	0.00	8,750.00	(8,750.00)	0.00%	0.00
Learning Resource Center	85,060.03	36,218.25	48,841.78	42.58%	23,155.38
Health Sciences Study Center	52,709.38	27,329.46	25,379.92	51.85%	21,825.22
Financial Aid-Clarendon	177,910.20	91,582.66	86,327.54	51.48%	66,078.83
Financial Aid-Pampa	47,347.87	25,133.94	22,213.93	53.08%	18,816.88
Financial Aid-Childress	51,948.93	28,052.68	23,896.25	54.00%	22,730.30
Registrar-Clarendon	88,614.00	43,347.95	45,266.05	48.92%	40,068.50
Admissions and Records-Clarendon	63,390.21	32,402.86	30,987.35	51.12%	53,082.61
Campus Security	57,000.00	24,076.25	32,923.75	42.24%	27,301.23
Board of Regents	14,000.00	4,417.01	9,582.99	31.55%	2,279.69
Executive Direction and Control	260,939.07	138,244.91	122,694.16	52.98%	110,862.44
Business and Fiscal Management-Clarendon	565,895.81	325,424.42	240,471.39	57.51%	296,432.23
Bus & Fiscal Mgmt - Pampa	66,157.82	26,817.66	39,340.16	40.54%	22,825.19
Bus & Fiscal Mgmt - Childress / Shamrock	35,300.00	9,362.90	25,937.10	26.52%	8,590.81
Computer Services	1,194,532.54	558,662.50	635,870.04	46.77%	425,401.71
Institutional Advancement	201,365.00	95,128.37	106,236.63	47.24%	102,293.12
Institutional Support	200,000.00	5,997.63	194,002.37	3.00%	1,349.14
Plant Administration & Support Services	488,155.24	331,944.58	156,210.66	68.00%	248,969.88
Transportation-Clarendon	171,580.33	54,374.04	117,206.29	31.69%	175,375.71
Transportation-Pampa	7,500.00	354.75	7,145.25	4.73%	550.08
Maintenance-Clarendon	553,936.89	483,453.64	70,483.25	87.28%	175,094.38
Maintenance - Pampa	111,002.84	10,130.58	100,872.26	9.13%	395,745.46
Maintenance - Childress	40,000.00	645.52	39,354.48	1.61%	7,777.95
Maintenance - Amarillo	12,000.00	3,823.75	8,176.25	31.86%	5,895.04
Major Repairs and Renovations	0.00	38,125.00	(38,125.00)	0.00%	16,539.69
Housekeeping-Clarendon	326,014.04	155,268.52	170,745.52	47.63%	121,700.24
Housekeeping-Pampa	60,140.72	28,015.95	32,124.77	46.58%	22,632.97
Housekeeping-Childress	14,000.00	6,669.99	7,330.01	47.64%	6,460.84
Housekeeping-Amarillo	3,500.00	1,290.49	2,209.51	36.87%	1,528.14
Grounds-Clarendon	74,186.60	28,565.47	45,621.13	38.50%	48,235.42
Grounds - Pampa	42,347.25	305.57	42,041.68	0.72%	7,856.66
Rent	98,362.50	49,381.25	48,981.25	50.20%	43,353.13
Utilities-Clarendon	295,000.00	125,403.65	169,596.35	42.51%	135,554.48
Utilities - Pampa	61,000.00	21,078.62	39,921.38	34.56%	29,159.50
Utilities - Childress	34,000.00	16,469.88	17,530.12	48.44%	15,134.13
Utilities - Amarillo	14,000.00	7,925.34	6,074.66	56.61%	5,547.96
Inter-fund Appropriations	2,402,439.96	64,749.67	2,337,690.29	2.70%	95,020.94
Expenses - Education and General	13,882,842.99	5,576,287.53	8,306,555.46	40.17%	4,960,876.17

	2025 Budget	2025 Actual	Balance	% of Budget Expense	2024 Actual
Revenue - Education and General	(13,922,739.48)	(11,142,417.06)	(2,780,322.42)	80.03%	(10,637,736.52)
Expense - Education and General	13,882,842.99	5,576,287.53	8,306,555.46	40.17%	4,960,876.17
Net Change to E & G Fund Balance	(39,896.49)	(5,566,129.53)	5,526,233.04	#####	(5,676,860.35)

Auxiliary Fund Budget

Revenue:

Bookstore	26,750.00	14,892.00	11,858.00	55.67%	17,023.73
Residence Halls	471,000.00	456,265.00	14,735.00	96.87%	451,360.00
Food Service	752,500.00	673,928.60	78,571.40	89.56%	656,664.65
Livestock & Equine Center	52,000.00	60,864.00	(8,864.00)	117.05%	0.00
Student Loans	0.00	0.00	0.00	0.00%	30.00
Sales and Services	2,700.00	1,421.65	1,278.35	52.65%	1,596.95
College House	8,400.00	4,200.00	4,200.00	50.00%	4,200.00
Miscellaneous Income	0.00	(228.60)	228.60	0.00%	5.58
Interfund Appropriations	1,875,787.39	0.00	1,875,787.39	0.00%	0.00
Revenue - Auxillary Fund	3,189,137.39	1,211,342.65	1,977,794.74	37.98%	1,130,880.91

Expense:

Bookstore	119,742.99	85,658.78	34,084.21	71.54%	78,650.61
Residence Halls	105,036.42	76,262.49	28,773.93	72.61%	40,021.38
Food Service	681,000.00	409,367.05	271,632.95	60.11%	542,763.26
Livestock & Equine Center	71,000.00	71,829.88	(829.88)	101.17%	19,210.68
Sales & Service	6,000.00	24.45	5,975.55	0.41%	57.09
Athletics - General	205,481.93	92,087.27	113,394.66	44.82%	47,938.20
Baseball	227,950.43	179,891.44	48,058.99	78.92%	184,307.57
Men's Basketball	176,724.70	150,487.23	26,237.47	85.15%	150,007.74
Women's Basketball	179,177.63	150,227.78	28,949.85	83.84%	143,581.93
Volleyball	134,294.74	95,113.09	39,181.65	70.82%	78,778.76
Softball	164,295.03	129,069.59	35,225.44	78.56%	120,115.01
Livestock/Meats Judging	305,242.52	259,792.52	45,450.00	85.11%	240,293.50
Intercollegiate Rodeo - Women's	130,127.17	77,848.92	52,278.25	59.83%	69,796.10
Intercollegiate Rodeo - Men's	299,706.93	178,697.53	121,009.40	59.62%	152,870.76
Ranch Horse Team	119,288.58	69,784.88	49,503.70	58.50%	60,199.54
Student Activities	21,000.00	6,125.73	14,874.27	29.17%	3,244.37
Institutional Scholarships	18,000.00	8,000.00	10,000.00	44.44%	0.00
Special Items	50,000.00	0.00	50,000.00	0.00%	0.00
Interfund Appropriations	342,690.07	0.00	342,690.07	0.00%	0.00

Expenses - Auxiliary Fund	3,356,759.14	2,040,268.63	1,316,490.51	60.78%	1,931,836.50
Revenue - Auxiliary Fund	(3,189,137.39)	(1,211,342.65)	(1,977,794.74)	37.98%	(1,130,880.91)
Expense - Auxiliary Fund	3,356,759.14	2,040,268.63	1,316,490.51	60.78%	1,931,836.50
Net Change to Auxiliary Fund Balance	167,621.75	828,925.98	(661,304.23)	494.52%	800,955.59

06 February Custodial Account Statements
Summary

Agency Account	Name	Owner	Ending Balance January 31, 2025	Ending Balance February 28, 2025	Net Activity 6
81-9171-00-00-2910	Century Club Agency	President - Mr Buckhaults	(2,350.54)	(2,191.30)	159.24
81-9050-00-00-2910	Ex-Students Agency	President - Mr Buckhaults	(1,047.67)	(1,050.68)	(3.01)
81-9053-00-00-2910	Ex-Student Courtyard - Agency	President - Mr Buckhaults	(762.80)	(764.99)	(2.19)
81-9060-02-00-2910	Miscellaneous-Agency-Miscellaneous	President - Mr Buckhaults	(3,273.92)	(3,273.92)	(9.35)
81-9080-00-00-2910	Returned Checks Agency Fund	President - Mr Buckhaults	(108.20)	(108.51)	(0.31)
81-9153-00-00-2910	Agency - Molly Goodnight Collegiate Chapter	President - Mr Buckhaults	(106.60)	(106.91)	(0.31)
81-9157-00-00-2910	Agency - Employee Scholarship Fund	President - Mr Buckhaults	(1,298.88)	(1,302.60)	(3.72)
81-9137-00-00-2910	Class 58-59	Pampa Dean - Mike Davis	(13,693.50)	(13,732.72)	(39.22)
81-9130-00-00-2910	National Tech Honor Society	Pampa Dean - Mike Davis	(26.01)	(26.08)	(0.07)
81-9104-02-00-2910	Student Government Assoc - Pampa	Pampa Dean - Mike Davis	(596.40)	(598.11)	(1.71)
81-9150-00-00-2910	Pampa Dean Agency	Pampa Dean - Mike Davis	(13,558.63)	(14,029.70)	(471.07)
81-9123-00-00-2910	Student Government Assoc	Will Thompson	(2,252.51)	(1,968.60)	283.91
81-9087-00-00-2910	Agency LEC	Rodeo Coach - Bret Franks	(2,238.27)	(2,244.69)	(6.42)
81-9059-00-00-2910	Rodeo Agency	Rodeo Coach - Bret Franks	(47,476.40)	(43,957.09)	3,519.31
81-9017-00-00-2910	Ranch Horse Team Agency-RANCH HORSE TEM	Rodeo Coach - Bret Franks / Holly Irish	(49,479.87)	(46,592.46)	2,887.41
81-9023-00-00-2910	Athletics-Men's Baseball-Agenc	Baseball Coach - Cory Russell	(15,966.74)	(16,012.47)	(45.73)
81-9026-00-00-2910	Athletics-Volleyball-Agency-Athletics - Volleyball	Volleyball Coach - Desiree Mamolejo	(11,905.87)	(11,939.98)	(34.11)
81-9010-00-00-2910	Athletics - Agency - Athletics	Women's Basketball Coach - Mark James	(17,615.37)	(17,929.94)	(314.57)
81-9020-00-00-2910	Athletics - Mens Basketball	Athletic Director - Mark James	(841.51)	(1,094.00)	(252.49)
81-9027-00-00-2910	Athletics-W Softball-Athletics - Women's Softball	Mens Basketball Coach - Blake Cochran	(9,134.77)	(9,411.05)	(276.28)
81-9031-00-00-2910	Block & Bridle-Agency-Block & Bridle	Softball Coach - Lindy Alexander	(15,850.54)	(10,073.93)	5,776.61
81-9110-00-00-2910	Nursing-White Caps-Agency-Voc Nursing - White Cap	Ranch Horse Coach - Holly Irish	(931.44)	(934.11)	(2.67)
81-9098-00-04-2910	Cosmetology Agency - Amarillo	Director of Nursing - Sherrie Denham	(9,651.15)	(9,678.80)	(27.65)
81-9098-00-01-2910	Cosmetology Student Scholarship Fund	Cosmetology Director - Decee Surratt	(11,270.91)	(12,637.90)	(1,366.99)
81-9098-00-00-2910	Cosmetology Agency-Pampa	Cosmetology Director - Decee Surratt	(757.48)	(759.65)	(2.17)
81-9043-00-00-2910	Cosmetology-Childress	Cosmetology Director - Decee Surratt	(19,238.64)	(19,509.49)	(270.85)
81-9066-00-00-2910	Drama Club-Agency-Drama Club	Cosmetology Director - Decee Surratt	(14,424.58)	(14,855.40)	(430.82)
81-9077-00-00-2910	Phi Theta Kappa-Agency-Phi Theta Kappa	Drama Instructor - Dr. Donahue	(2,349.14)	(2,355.87)	(6.73)
81-9056-00-00-2910	Judging - Meat Judging	Drama Instructor - Dr. Donahue	(1,016.65)	(1,019.56)	(2.91)
81-9057-00-00-2910	Judging Team-Agency-Judging Team	Judging Director - Johnny Treichel	(1,033.27)	(1,036.23)	(2.96)
81-9055-00-00-2910	Judging Contest-Contest	Judging Director - Johnny Treichel	(144,177.86)	(75,017.26)	69,160.60
81-9074-00-00-2910	RFO-Agency-Ranch and Feedlot Operations	Judging Director - Johnny Treichel	(52,268.83)	(410.15)	(410.15)
81-9077-00-00-2910	RFO-WRCF-Agency	RFO Director - Tye Chesser	(34,089.63)	(52,436.89)	(168.06)
81-9120-00-00-2910	Student Life Agency	RFO Director - Tye Chesser	(191.91)	(34,208.90)	(119.27)
81-9147-00-00-2910	Agency - Student Fines / Resident Hall Repair Agency	Director of Student Life - Mitchell Parker	(41,610.79)	(192.46)	(0.55)
81-9145-00-00-2910	CDL Relief Fund	Director of Student Life - Mitchell Parker	(468.18)	(43,485.20)	(1,874.41)
81-9143-00-00-2910	Welding Agency	CDL Director - Casey Upton	(1,582.13)	(469.52)	(1.34)
81-9156-00-00-2910	Paws Against Cancer	Welding Instructor - Mark Simmons	(6,910.77)	(1,582.65)	(4.52)
		Brandi Havens	(551,545.01)	(6,934.38)	(23.61)
		Total Agency		(475,934.15)	75,610.86

NEGATIVE = INCOME
POSITIVE = EXPENSE

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
HERRING NATIONAL BANK	STOP PMT CK#8399	2/4/2025	STOP PMT#8399	\$15.00	OPERATING
AWESOME WATER SOLUTIONS	8594	2/5/2025	REPAIR LEAK BEHIND CC MAINTBLD	\$1,033.98	OPERATING
BRANDON PORTER, JR.	8595	2/5/2025	WBB OFFICIAL 1/30/25	\$190.00	OPERATING
CHRIS MATTHEWS	8596	2/5/2025	REIMBURSE RFIA TRAINING	\$200.00	OPERATING
CITY OF AMARILLO	8597	2/5/2025	JAN 2025 AMARILLO WATER	\$277.27	OPERATING
CITY OF CLARENDON	8598	2/5/2025	JAN 2025 CC WATER & TRASH	\$4,283.78	OPERATING
COLIN CROMEENS	8599	2/5/2025	MBB OFFICIAL 1/30/25	\$190.00	OPERATING
DONLEY CO. TAX ASSESSOR-COLLECTOR	8600	2/5/2025	WINDOW TAGS 7 FLEET VEHICLES	\$52.50	OPERATING
ELLIOTT ELECTRIC SUPPLY, INC.	8601	2/5/2025	LIGHT BULBS FOR PAMPA CAMPUS	\$525.00	OPERATING
GRAINGER	8602	2/5/2025	KEY BLANKS FOR CC CAMPUS	\$67.86	OPERATING
HD SUPPLY	8603	2/5/2025	REGENTS HVAC PARTS	\$673.54	OPERATING
HD SUPPLY	8603	2/5/2025	CC CAMPUS SPACE HEATERS	\$134.60	OPERATING
JEFFREY PAUL BERRYMAN	8604	2/5/2025	BB UMPIRE 2/1/2025	\$380.00	OPERATING
JEREMIAH BRETONES	8605	2/5/2025	MBB REF 1/23/2025	\$190.00	OPERATING
JOHNNY TREICHEL	8606	2/5/2025	MEATS MEALS@HEREFORD 2/18-22	\$780.00	OPERATING
JOHNNY TREICHEL	8607	2/5/2025	LSTOCK MEALS@SAN ANTONIO	\$1,120.00	OPERATING
HOLIDAY MOTOR COACH, LLC	8608	2/5/2025	MBB CHARTER ROSWELL 1/27/25	\$3,228.00	OPERATING
SCOTT L. CAMPBELL	8609	2/5/2025	WBB/MBB GYM SECURITY 1/30/25	\$200.00	OPERATING
THE PAMPA NEWS	8610	2/5/2025	JAN 2025 PAMPA NEWS ADS	\$331.00	OPERATING
TREVER PHILLIPS	8611	2/5/2025	MBB REF 2/3/2025	\$190.00	OPERATING
BROLLIER'S AUTO PARTS	8612	2/5/2025	JAN 2025 CC GROUNDS SUPPLIES	\$167.02	OPERATING
BROLLIER'S AUTO PARTS	8612	2/5/2025	JAN 2025 AUTO DEPT SUPPLIES	\$659.80	OPERATING
XCEL ENERGY	8613	2/5/2025	JAN 2025 PAMPA ELECTRIC	\$1,130.48	OPERATING
XCEL ENERGY	8613	2/5/2025	JAN 2025 PAMPA WELL ELECTRIC	\$167.80	OPERATING
CLARENDON COLLEGE	CHGBACK SP-25 STU	2/5/2025	CHARGEBACK S CHRISTOPHER	\$682.44	OPERATING
287 AG, LLC.	EFT0000000002929	2/5/2025	LEC FEED FOR STOCK	\$1,533.00	OPERATING
ALLSTATE SECURITY INDUSTRIES, INC.	EFT0000000002930	2/5/2025	CC SECURITY 1/20-26/2025	\$1,237.50	OPERATING
AMA TECHTEL COMMUNICATIONS	EFT0000000002931	2/5/2025	FEB 2025 PAMPA PHONE SVC	\$427.56	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
AquaOne	EFT000000002932	2/5/2025	JAN25/AMA BOTTLE DISPENSOR	\$10.99	OPERATING
BRADY LONG	EFT000000002933	2/5/2025	BB UMPIRE 2/1/2025	\$380.00	OPERATING
BRAXTON BATES	EFT000000002934	2/5/2025	MBB OFFICIAL 1/30/25	\$190.00	OPERATING
BRAXTON BATES	EFT000000002934	2/5/2025	MBB OFFICIAL 1/16/25	\$190.00	OPERATING
CHIEF PLASTIC PIPE & SUPPLY INC.	EFT000000002935	2/5/2025	PAMPA KITCHEN SINK REPAIR	\$52.72	OPERATING
COLEMAN M. HASIE	EFT000000002936	2/5/2025	MBB OFFICIAL 1/23/25	\$190.00	OPERATING
COLEMAN M. HASIE	EFT000000002936	2/5/2025	MBB OFFICIAL 2/3/25	\$190.00	OPERATING
CORNELL'S COUNTRY STORE	EFT000000002937	2/5/2025	LEC STOCK/MAXI GAIN	\$296.94	OPERATING
DAVID MOORE	EFT000000002938	2/5/2025	WBB OFFICIAL 1/30/2025	\$190.00	OPERATING
DAVID RASMUSSEN	EFT000000002939	2/5/2025	MBB REF 1/23/25	\$190.00	OPERATING
EMPIRE PAPER COMPANY	EFT000000002940	2/5/2025	JAN 2025 PAMPA CUSTODIAL SUPP	\$711.47	OPERATING
EMPIRE PAPER COMPANY	EFT000000002940	2/5/2025	JAN 2025 AMA CUSTODIAL SUPP	\$443.81	OPERATING
EMPIRE PAPER COMPANY	EFT000000002940	2/5/2025	JAN 2025 CC CUSTODIAL SUPPLIES	\$1,075.87	OPERATING
EAN SERVICES, LLC	EFT000000002941	2/5/2025	JAN 2025 FLEET VEHICLE LEASE	\$923.12	OPERATING
EAN SERVICES, LLC	EFT000000002941	2/5/2025	DEC 2024 FLEET VEHICLE LEASE	\$923.12	OPERATING
FLOYD'S AUTO SUPPLY ACCT#610	EFT000000002942	2/5/2025	JAN 2025 AUTO DEPT SUPPLIES	\$170.75	OPERATING
FLOYD'S AUTO SUPPLY ACCT#610	EFT000000002942	2/5/2025	TIRE REPAIR/LEC SKID STEER	\$120.56	OPERATING
FLOYD'S AUTO SUPPLY ACCT#610	EFT000000002942	2/5/2025	3 NEW TIRES/LEC STOCK TRAILER	\$885.55	OPERATING
FLOYD'S AUTO SUPPLY ACCT#610	EFT000000002942	2/5/2025	JAN 2025 CC GROUNDS SUPPLIES	\$6.49	OPERATING
GREAT WESTERN DINING SERVICE	EFT000000002943	2/5/2025	BOARD BILLING WE 1/29/25	\$18,436.32	OPERATING
GREAT WESTERN DINING SERVICE	EFT000000002943	2/5/2025	FOOD LOSS/CAF WALKIN DOWN	\$333.11	OPERATING
GREENLIGHT GAS #3955	EFT000000002944	2/5/2025	JAN 2025 CC CAMPUS GAS	\$7,660.86	OPERATING
JEREMY WADE BROWN	EFT000000002945	2/5/2025	WBB OFFICIAL 1/30/2025	\$190.00	OPERATING
JIMMY GAUNA	EFT000000002946	2/5/2025	SB UMPIRE 1/27/2025	\$360.00	OPERATING
JOHNNIE PETTIE, JR	EFT000000002947	2/5/2025	SB UMPIRE 1/27/2025	\$360.00	OPERATING
MBS DIRECT	EFT000000002948	2/5/2025	SP-24 FAIDE STUDENT BOOK	\$249.62	OPERATING
JAMES MICHAEL DAVIS	EFT000000002949	2/5/2025	REIMB/PRISONER MEALS @PAMPA	\$114.64	OPERATING
MIKE YELL	EFT000000002950	2/5/2025	MBB REF 1/30/2025	\$190.00	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
MIKE YELL	EFT000000002950	2/5/2025	MBB REF 1/16/2025	\$190.00	OPERATING
MIKE YELL	EFT0000000002950	2/5/2025	MBB REF 2/3/2025	\$190.00	OPERATING
QUARLES PETROLEUM #861314771	EFT0000000002951	2/5/2025	JAN 2025 FLEET VEHICLES FUEL	\$2,589.83	OPERATING
RUN BUSINESS SOLUTIONS	EFT0000000002952	2/5/2025	SONIC FIREWALL SVC RENEWAL	\$548.41	OPERATING
SYNTRIO SOLUTIONS, LLC.	EFT0000000002953	2/5/2025	FEB 2025 CHILDRESS WIFI	\$339.24	OPERATING
SPROUSE SHRADER SMITH PLLC	EFT0000000002954	2/5/2025	DEC 2024 LEGAL FEES	\$500.00	OPERATING
THE CLARENDON ENTERPRISE	EFT0000000002955	2/5/2025	JAN25/ENTERPRISE "D" WEB ADS	\$75.00	OPERATING
VERIFIED FIRST BACKGROUND SVCS	EFT0000000002956	2/5/2025	2 EMPLOYEE BACKGROUND CHECKS	\$108.82	OPERATING
WHITNEY RUSSELL PRINTERS	EFT0000000002957	2/5/2025	80 SB POSTER/SCHEDULES	\$72.59	OPERATING
YourNewSchool	EFT0000000002958	2/5/2025	SP-25 CHILD COMSO NAIL SUPPLI	\$105.36	OPERATING
YourNewSchool	EFT0000000002958	2/5/2025	SP-25 PAMPA COSMO NAIL SUPPLIE	\$105.36	OPERATING
YourNewSchool	EFT0000000002958	2/5/2025	SP 025 AMA COSMO NAIL SUPPLIES	\$105.36	OPERATING
ZACHARY NOLAND	EFT0000000002959	2/5/2025	MBB REF 1/16/2025	\$190.00	OPERATING
VISA	B.COCHRAN 2/6/2025	2/6/2025	MBB UNIFORMS LAUNDRY DETERGENT	\$15.10	OPERATING
VISA	B.COCHRAN 2/6/2025	2/6/2025	MBB TEAM MEAL 2/3/2025	\$30.35	OPERATING
VISA	B.FRANKS 2/6/2025	2/6/2025	JAN 2025 BRET/FUEL/HAUL STOCK	\$272.14	OPERATING
VISA	C.RUSSELL 2/6/2025	2/6/2025	MAILING BB RECRUIT SHIRTS/HATS	\$73.01	OPERATING
VISA	C.UPTON 2/6/2025	2/6/2025	CDL STUDENT EXAM FEE	\$81.00	OPERATING
VISA	DRIVER#2 2/6/2025	2/6/2025	MEATS TEAM@FT WORTH 1/28-2/3	\$1,353.07	OPERATING
VISA	M.JAMES 2/6/2025	2/6/2025	GYM CONCESSION STAND SUPPLIES	\$197.70	OPERATING
VISA	M.JAMES 2/6/2025	2/6/2025	WBB TEAM MEAL 2/3/2025	\$63.00	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	RFO/UNDER DESK FILE CABINET	\$102.37	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	CINDY NAME CHANGE/NOTARY STAMP	\$34.54	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	PAMPA WELDING POWER GRINDERS	\$179.95	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	MITCH/NORDIC COOKIE STAMPS	\$28.00	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	MITCH/ SMORE & POPCORN MAKERS	\$251.95	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	CC WELDING POWER GRINDERS	\$199.95	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	50" TV FOR DIGITAL SIGNAGE	\$239.99	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
VISA	VISA#1 2/6/2025	2/6/2025	CC WELDING EAR PLUGS	\$22.90	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	ALL COSMO/AMAZON SUPPLIES	\$1,422.28	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	SB PA SYSTEM SPEAKERS	\$399.00	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	JAN 2025 SHOPIFY SHIPPING	\$9.45	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	TYSON PATE COMPUTER SPEAKERS	\$21.11	OPERATING
VISA	VISA#1 2/6/2025	2/6/2025	100 PCS CATS/6 PASSTHROUGH	\$22.96	OPERATING
VISA	VISA#3 2/6/2025	2/6/2025	SGA MEALS/FUEL@AUSTIN 2/1-4	\$290.25	OPERATING
VISA	W.SMITH 2/6/2025	2/6/2025	WYATT/FUEL TO HAUL STOCK	\$318.55	OPERATING
AUTOMATIC PAYROLL SYSTEMS, INC.	JAN25/PAYROLL FEES	2/7/2025	JAN 2025 APS PAYROLL FEES	\$2,950.00	OPERATING
ARLUSS CORLISS	8614	2/11/2025	LODGING EXPENSE/MEATS TEAM	\$190.00	OPERATING
VERNON COLLEGE	8615	2/11/2025	VB ENTRY FEE 9/2-3 @VERNON	\$200.00	OPERATING
TX COMPROLLER OF PUBLIC ACCTS	JAN 2025 SALES TAX	2/11/2025	JAN 2025 SALES TAX	\$19,511.39	OPERATING
ARMSTRONG MCCALL BEAUTY SUPPLY	8616	2/12/2025	AMARILLO COSMO SUPPLIES	\$201.88	OPERATING
BRET FRANKS	8617	2/12/2025	M.RODEO TRAVEL \$ /ODESSA	\$700.00	OPERATING
CIRCLE N APPLIANCE	8618	2/12/2025	WASHER & DRYER FOR DORMS	\$2,932.00	OPERATING
CITY OF CHILDRESS	8619	2/12/2025	JAN 2025 CHILDRESS WATER	\$363.40	OPERATING
ECOLAB INC	8620	2/12/2025	FEB 2025 CAF DISHWASHER	\$175.85	OPERATING
ELLIOTT ELECTRIC SUPPLY, INC.	8621	2/12/2025	15W LED BULBS/CC CAMPUS	\$525.00	OPERATING
HD SUPPLY	8622	2/12/2025	HVAC MOTORS@REGENTS HALL	\$336.77	OPERATING
HEMPHILL COUNTY EXTENSION SERVICE	8623	2/12/2025	RFO/HEMPHILL FIRE PREPAREDNESS	\$675.00	OPERATING
HERRING NATIONAL BANK	8624	2/12/2025	JAN 2025 REFUND FEES	\$76.80	OPERATING
JOHNNY ATWOOD	8626	2/12/2025	WBB OFFICIAL 2/3/2025	\$190.00	OPERATING
JOHNNY TREICHEL	8627	2/12/2025	MEATS MEALS@HOUSTON 3/4-9	\$1,300.00	OPERATING
JOHNNY TREICHEL	8628	2/12/2025	L STOCK MEALS@HOUSTON 3/12-18	\$1,400.00	OPERATING
KELSEY CURRY	8629	2/12/2025	WBB OFFICIAL 2/3/2025	\$190.00	OPERATING
RMA TOLL PROCESSING	8630	2/12/2025	MICHAEL/TOLLS/SACS CONF	\$2.04	OPERATING
BIG INNING, INC.	8631	2/12/2025	SB TEAM PANTS & SOCKS	\$4,195.00	OPERATING
SIERRA SPRINGS	8632	2/12/2025	JAN2025 CHILDRESS BOTTLE WATER	\$46.44	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
SOUTHWESTERN ELECTRIC POWER	8633	2/12/2025	FEB25/PRES SHOP ELECTRIC	\$15.88	OPERATING
SOUTHWESTERN ELECTRIC POWER	8633	2/12/2025	FEB25/VO-TECH ELECTRIC	\$71.24	OPERATING
SOUTHWESTERN ELECTRIC POWER	8633	2/12/2025	FEB25/PRES HOUSE ELECTRIC	\$239.91	OPERATING
SPORTS ATTACK	8634	2/12/2025	BB HACK ATTACK MOTOR	\$320.00	OPERATING
LINDE GAS & EQUIPMENT, INC	8635	2/12/2025	PAMPA WELDING/GRINDING WHEEL	\$24.37	OPERATING
WINSUPPLY OF AMARILLO	8636	2/12/2025	REGENTS WEST HOT WATER HEATER	\$5,851.32	OPERATING
WYATT SMITH	8637	2/12/2025	W.RODEO TRAVEL \$/ODESSA	\$500.00	OPERATING
Ivan Aguilar	8638	2/12/2025	Check Refund	\$1,390.00	OPERATING
Chaurdae Gilmore	8639	2/12/2025	Check Refund	\$1,441.00	OPERATING
Lindsey Autumn Carpenter	8640	2/12/2025	Check Refund	\$1,005.00	OPERATING
Jaimi Rae'Ann Chute	8641	2/12/2025	Check Refund	\$873.00	OPERATING
Joseline Madrid	8642	2/12/2025	Check Refund	\$956.00	OPERATING
Vanessa Flores	8643	2/12/2025	Check Refund	\$5,184.00	OPERATING
Gloria Flores	8644	2/12/2025	Check Refund	\$4,657.00	OPERATING
Helene Denay Simpkins	8645	2/12/2025	Check Refund	\$5,096.00	OPERATING
Kalmine Shanell Menson	8646	2/12/2025	Check Refund	\$1,441.00	OPERATING
Aracely Nicole Caldera	8647	2/12/2025	Check Refund	\$954.00	OPERATING
Karcynn Mackynzie Pierce	8648	2/12/2025	Check Refund	\$3,004.82	OPERATING
Madison Paige Moffett	8649	2/12/2025	Check Refund	\$104.00	OPERATING
Kensie Drew Kimball	8650	2/12/2025	Check Refund	\$371.00	OPERATING
Jodee Wayne Pigg	8651	2/12/2025	Check Refund	\$432.19	OPERATING
Yanci Deene Hutchison	8652	2/12/2025	Check Refund	\$3,491.00	OPERATING
Madilyn Grace Armstrong	8653	2/12/2025	Check Refund	\$4,053.00	OPERATING
Lyndsey Bivins	8654	2/12/2025	Check Refund	\$1,969.00	OPERATING
Nicole Schumacher	8655	2/12/2025	Check Refund	\$1,437.00	OPERATING
Carmen Alicia Vela	8656	2/12/2025	Check Refund	\$1,528.00	OPERATING
Adriana Victoria Araujo	8657	2/12/2025	Check Refund	\$2,229.00	OPERATING
Jada Jones	8658	2/12/2025	Check Refund	\$1,844.00	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Aspen Brett Miller	8659	2/12/2025	Check Refund	\$148.00	OPERATING
Aspen Brett Miller	8659	2/12/2025	Check Refund	\$1,973.36	OPERATING
Angelina Alcozer	8660	2/12/2025	Check Refund	\$1,467.00	OPERATING
Joshua Aaron Booth	8661	2/12/2025	Check Refund	\$4,284.00	OPERATING
Antonio Gray Soria	8662	2/12/2025	Check Refund	\$2,671.00	OPERATING
Josiah Ethan Smith	8663	2/12/2025	Check Refund	\$100.00	OPERATING
Dario Castillo Gamez	8664	2/12/2025	Check Refund	\$1,708.00	OPERATING
Leaja S Neese	8665	2/12/2025	Check Refund	\$3,926.00	OPERATING
Boyce Mark Jason Kraut	8666	2/12/2025	Check Refund	\$1,059.00	OPERATING
Cole Fredrick Simon	8667	2/12/2025	Check Refund	\$826.00	OPERATING
David Gonzalos Cervantes	8668	2/12/2025	Check Refund	\$1,011.00	OPERATING
Brinley Madison Pugh	8669	2/12/2025	Check Refund	\$1,830.00	OPERATING
Audrey B Townzen	8670	2/12/2025	Check Refund	\$822.00	OPERATING
Alexa P Trejo	8671	2/12/2025	Check Refund	\$750.00	OPERATING
Courtlyn Cole Conkin	8672	2/12/2025	Check Refund	\$700.00	OPERATING
Emmalyne Grace Roys	8673	2/12/2025	Check Refund	\$1,000.00	OPERATING
Cambree Taylor Brown	8674	2/12/2025	Check Refund	\$511.83	OPERATING
Jennifer R Clayton	8675	2/12/2025	Check Refund	\$2,925.00	OPERATING
Adicyn Jo Martin	8676	2/12/2025	Check Refund	\$150.00	OPERATING
Clarissa Elena Gamboa	8677	2/12/2025	Check Refund	\$1,813.00	OPERATING
Clarissa Lisette Lepe	8678	2/12/2025	Check Refund	\$3,228.00	OPERATING
Grace Marie Baggett	8679	2/12/2025	Check Refund	\$900.00	OPERATING
Robert Luis De Jesus Martinez	8680	2/12/2025	Check Refund	\$162.00	OPERATING
Laney Dawn Rummel	8681	2/12/2025	Check Refund	\$4,312.00	OPERATING
Erin Iizann Allen	8682	2/12/2025	Check Refund	\$996.00	OPERATING
Brooklynn Breeann Williams	8683	2/12/2025	Check Refund	\$5,344.00	OPERATING
Shelby Elizabeth Carter	8684	2/12/2025	Check Refund	\$437.00	OPERATING
Neera Erlinda Samora	8685	2/12/2025	Check Refund	\$1,437.00	OPERATING

Clarendon College**Checks Written****February, 2025****Vendor Name**

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Finnegan Shawn Johnston	8686	2/12/2025	Check Refund	\$3,820.00	OPERATING
Iziak Trent Weatherread	8687	2/12/2025	Check Refund	\$4,597.00	OPERATING
Iziak Trent Weatherread	8687	2/12/2025	Check Refund	\$774.00	OPERATING
Alexis Rene Gardenhire	8688	2/12/2025	Check Refund	\$1,500.31	OPERATING
Brighton Alan Wooton	8689	2/12/2025	Check Refund	\$451.30	OPERATING
Rye McCall Reynolds	8690	2/12/2025	Check Refund	\$2,529.00	OPERATING
Rebecca Renee Earls	8691	2/12/2025	Check Refund	\$437.00	OPERATING
Sydne Raeh Victor	8692	2/12/2025	Check Refund	\$3,447.00	OPERATING
Isabela Maria Pinheiro Correia Gomes	8693	2/12/2025	Check Refund	\$300.00	OPERATING
Ashlee Holmes	8694	2/12/2025	Check Refund	\$5,163.00	OPERATING
Landry Jake Miller	8695	2/12/2025	Check Refund	\$2,404.00	OPERATING
Gage Wyatt Whatley	8696	2/12/2025	Check Refund	\$4,024.00	OPERATING
Addison Brooke Koontz	8697	2/12/2025	Check Refund	\$1,181.00	OPERATING
James Coltt McAllister	8698	2/12/2025	Check Refund	\$200.00	OPERATING
Nashia Yvonne Coleman	8699	2/12/2025	Check Refund	\$598.00	OPERATING
Henry Samuel Sutton	8700	2/12/2025	Check Refund	\$4,864.00	OPERATING
Connor Ezekiel Porath	8701	2/12/2025	Check Refund	\$1,354.00	OPERATING
Gidaya Idnam Dobbins	8702	2/12/2025	Check Refund	\$1,493.00	OPERATING
Lydia Sharp	8703	2/12/2025	Check Refund	\$846.00	OPERATING
Hailee Addyson Cunningham	8704	2/12/2025	Check Refund	\$1,041.00	OPERATING
Dustin Scott Phillips	8705	2/12/2025	Check Refund	\$37.00	OPERATING
Shaylee May Warner	8706	2/12/2025	Check Refund	\$3,217.00	OPERATING
Madilynn H Nichols	8707	2/12/2025	Check Refund	\$137.00	OPERATING
Allysondra Dianne Bowers	8708	2/12/2025	Check Refund	\$1,014.00	OPERATING
Ana Cristina Vieira	8709	2/12/2025	Check Refund	\$175.00	OPERATING
Chrissy Jeanette Branscum	8710	2/12/2025	Check Refund	\$3,266.00	OPERATING
Takyr Lee Goree	8711	2/12/2025	Check Refund	\$1,403.00	OPERATING
Angel Damian Tinajero	8712	2/12/2025	Check Refund	\$425.00	OPERATING

Clarendon College**Checks Written****February, 2025**

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Taleeyah Lanae Glynn	8713	2/12/2025	Check Refund	\$356.25	OPERATING
Raelynn A Stephenson	8714	2/12/2025	Check Refund	\$3,236.00	OPERATING
Matthew Val McLanahan	8715	2/12/2025	Check Refund	\$114.00	OPERATING
Kaden A Widacki	8716	2/12/2025	Check Refund	\$189.00	OPERATING
Anthony Ortiz	8717	2/12/2025	Check Refund	\$546.78	OPERATING
Kennadie Leigh Cummins	8718	2/12/2025	Check Refund	\$51.18	OPERATING
Tandie Renae Cummins	8719	2/12/2025	Check Refund	\$51.18	OPERATING
Aubrynn Kate Bichsel	8720	2/12/2025	Check Refund	\$230.61	OPERATING
Morgan Faith Johnston	8721	2/12/2025	Check Refund	\$200.00	OPERATING
Haylie Anisa Enriquez	8722	2/12/2025	Check Refund	\$1,193.00	OPERATING
Hoyt Wayne Roff	8723	2/12/2025	Check Refund	\$3,486.00	OPERATING
Naileli DeLayna Rodriguez	8724	2/12/2025	Check Refund	\$495.00	OPERATING
Celia Sylvia Stanghellini	8725	2/12/2025	Check Refund	\$170.61	OPERATING
Kolby Donovan Burton	8726	2/12/2025	Check Refund	\$1,242.00	OPERATING
Krysta Mari Cook	8727	2/12/2025	Check Refund	\$3,408.00	OPERATING
Michael Josiah Fuentes	8728	2/12/2025	Check Refund	\$1,073.00	OPERATING
Jessie Ray Ramos	8729	2/12/2025	Check Refund	\$258.78	OPERATING
Degan Blaine Barnes	8730	2/12/2025	Check Refund	\$230.61	OPERATING
Elizabeth Chatman	8731	2/12/2025	Check Refund	\$897.00	OPERATING
Ketreonna Laneshia Branch	8732	2/12/2025	Check Refund	\$961.00	OPERATING
Israel Ortega	8733	2/12/2025	Check Refund	\$812.56	OPERATING
Erika Shae Maness	8734	2/12/2025	Check Refund	\$5,135.00	OPERATING
Courtney Jayde Auhl	8735	2/12/2025	Check Refund	\$194.00	OPERATING
Trevor Jacob Christensen	8736	2/12/2025	Check Refund	\$2,853.00	OPERATING
Shawn Alan Crutcher	8737	2/12/2025	Check Refund	\$1,734.77	OPERATING
Wendie Nichole Emmons	8738	2/12/2025	Check Refund	\$5,466.39	OPERATING
Velora Villarreal	8739	2/12/2025	Check Refund	\$6,472.00	OPERATING
Laci E Newlin	8740	2/12/2025	Check Refund	\$1,862.00	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Patrick James Monds	8741	2/12/2025	Check Refund	\$1,837.00	OPERATING
Jah Re'Seyon Gulley	8742	2/12/2025	Check Refund	\$4,264.00	OPERATING
Samuel Perez	8743	2/12/2025	Check Refund	\$69.00	OPERATING
Zane Michael Clark	8744	2/12/2025	Check Refund	\$898.25	OPERATING
Chelsea Joy Clark	8745	2/12/2025	Check Refund	\$60.00	OPERATING
Lynde Taylor Yannis	8746	2/12/2025	Check Refund	\$762.00	OPERATING
Yamilet Yanet Granados	8747	2/12/2025	Check Refund	\$917.38	OPERATING
Sandra Rose Martinez	8748	2/12/2025	Check Refund	\$2,171.00	OPERATING
Autumn Michelle Captain	8749	2/12/2025	Check Refund	\$6,580.00	OPERATING
Isavel Ramirez	8750	2/12/2025	Check Refund	\$2,163.00	OPERATING
Deisi Mendoza	8751	2/12/2025	Check Refund	\$1,393.00	OPERATING
Hagan O'Donnell	8752	2/12/2025	Check Refund	\$1,440.00	OPERATING
Creed Hughes	8753	2/12/2025	Check Refund	\$1,572.25	OPERATING
Aletha Angel Usanga	8754	2/12/2025	Check Refund	\$2,199.00	OPERATING
Micaela Nicole Nunez	8755	2/12/2025	Check Refund	\$2,531.00	OPERATING
Kaitlin Nicole Rodriguez	8756	2/12/2025	Check Refund	\$945.00	OPERATING
Josee Smith	8757	2/12/2025	Check Refund	\$1,294.00	OPERATING
Emily Jaramillo	8758	2/12/2025	Check Refund	\$2,040.00	OPERATING
Anabelle Sariah Martinez	8759	2/12/2025	Check Refund	\$2,223.00	OPERATING
Maci Crisp	8760	2/12/2025	Check Refund	\$7,186.00	OPERATING
Aubrey Renae Meador	8761	2/12/2025	Check Refund	\$5,397.00	OPERATING
Carter Martin Munson	8762	2/12/2025	Check Refund	\$450.00	OPERATING
Ezekiel Coneway	8763	2/12/2025	Check Refund	\$1,500.00	OPERATING
Hilary Heather Scott	8764	2/12/2025	Check Refund	\$4,647.00	OPERATING
Ritchlyn Anderson	8765	2/12/2025	Check Refund	\$3,010.00	OPERATING
Nathan Ian Hill	8766	2/12/2025	Check Refund	\$300.00	OPERATING
Rhianna N Miranda	8767	2/12/2025	Check Refund	\$2,138.00	OPERATING
Mason Lee Erickson	8768	2/12/2025	Check Refund	\$3,847.00	OPERATING

Clarendon College**Checks Written****February, 2025**

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Rodrigo Magadan	8769	2/12/2025	Check Refund	\$1,969.00	OPERATING
Teagan Elaine Taylor	8770	2/12/2025	Check Refund	\$1,492.00	OPERATING
Alycia Raelyn McInturf	8771	2/12/2025	Check Refund	\$703.38	OPERATING
Baylee Marr	8772	2/12/2025	Check Refund	\$64.00	OPERATING
Parker Jo Fry	8773	2/12/2025	Check Refund	\$313.00	OPERATING
Shelby Aveanne Martin	8774	2/12/2025	Check Refund	\$1,438.00	OPERATING
Jake Reid Lamb	8775	2/12/2025	Check Refund	\$7,476.00	OPERATING
Julianna K Liles	8776	2/12/2025	Check Refund	\$502.00	OPERATING
Shonise Meekins	8777	2/12/2025	Check Refund	\$6,580.00	OPERATING
Wyatt Douglas Williams	8778	2/12/2025	Check Refund	\$12,755.00	OPERATING
Adriano Lee Miranda	8779	2/12/2025	Check Refund	\$675.00	OPERATING
Mitchell Dewayne Pace	8780	2/12/2025	Check Refund	\$85.00	OPERATING
Synia L Roberts	8781	2/12/2025	Check Refund	\$530.00	OPERATING
Tatiana Deann Houston	8782	2/12/2025	Check Refund	\$1,966.00	OPERATING
Lyndee Nichole Debose	8783	2/12/2025	Check Refund	\$2,480.00	OPERATING
Karlee Rae Lutz	8784	2/12/2025	Check Refund	\$1,050.00	OPERATING
Mackenzie Dell Abbott	8785	2/12/2025	Check Refund	\$2,791.00	OPERATING
Barbara Micheal Martin	8786	2/12/2025	Check Refund	\$984.00	OPERATING
Riley Barber	8787	2/12/2025	Check Refund	\$135.00	OPERATING
Warren T Mays	8788	2/12/2025	Check Refund	\$2,628.00	OPERATING
Railey Chase Nieto	8789	2/12/2025	Check Refund	\$1,980.00	OPERATING
Jacoby Dean Seabourn	8790	2/12/2025	Check Refund	\$3,069.00	OPERATING
Cayden Rose Caston	8791	2/12/2025	Check Refund	\$734.00	OPERATING
Evan Lee Jones	8792	2/12/2025	Check Refund	\$776.50	OPERATING
Addyson Parker Hale	8793	2/12/2025	Check Refund	\$1,477.00	OPERATING
Sierra Leandress Washington	8794	2/12/2025	Check Refund	\$3,250.00	OPERATING
Natalie Marie Pineda	8795	2/12/2025	Check Refund	\$1,689.00	OPERATING
Ronin Eryk DeMaroney	8796	2/12/2025	Check Refund	\$4,853.00	OPERATING

Clarendon College**Checks Written****February, 2025****Vendor Name**

Jennifer Yanez Lopez	8797	2/12/2025	Check Refund	Applied Amount	Checkbook ID
				\$1,438.00	OPERATING
Andrew Dietrich	8798	2/12/2025	Check Refund		\$170.61 OPERATING
Luke Douglas Asiala	8799	2/12/2025	Check Refund		\$59.00 OPERATING
Jarren Andrew Hill	8800	2/12/2025	Check Refund		\$39.39 OPERATING
Brady Austin Brooks	8801	2/12/2025	Check Refund		\$684.00 OPERATING
Seniya Nicole Wilson	8802	2/12/2025	Check Refund		\$1,583.00 OPERATING
Mario Alberto Garcia	8803	2/12/2025	Check Refund		\$1,737.00 OPERATING
Antonia Margie Deleon	8804	2/12/2025	Check Refund		\$1,738.00 OPERATING
Brinkley Ann Williams	8805	2/12/2025	Check Refund		\$4,988.00 OPERATING
Alyssa Marie Rodriguez	8806	2/12/2025	Check Refund		\$357.00 OPERATING
Peyton Blaine Blackmon	8807	2/12/2025	Check Refund		\$133.20 OPERATING
John Clancey Newman	8808	2/12/2025	Check Refund		\$73.00 OPERATING
Jillian Parker Pierce	8809	2/12/2025	Check Refund		\$90.00 OPERATING
Sydney Hatfield	8810	2/12/2025	Check Refund		\$497.00 OPERATING
Furie Sioux Barber	8811	2/12/2025	Check Refund		\$100.00 OPERATING
Collin Ace Garcia	8812	2/12/2025	Check Refund		\$90.00 OPERATING
Mason Overmiller	8813	2/12/2025	Check Refund		\$90.00 OPERATING
Mya Nicole Edwards	8814	2/12/2025	Check Refund		\$3,435.00 OPERATING
Vincent Robert Sherwood	8815	2/12/2025	Check Refund		\$1,997.00 OPERATING
Klaryssa Nicole Casares	8816	2/12/2025	Check Refund		\$1,438.00 OPERATING
Jonathan Gage Finley	8817	2/12/2025	Check Refund		\$1,325.00 OPERATING
Monique Cecelia Brown	8818	2/12/2025	Check Refund		\$1,583.00 OPERATING
Breannah Hailee Bryne	8819	2/12/2025	Check Refund		\$1,438.00 OPERATING
Jeremiah Poulos-Crawford	8820	2/12/2025	Check Refund		\$1,426.00 OPERATING
Micha Maire Holloway	8821	2/12/2025	Check Refund		\$1,043.36 OPERATING
Justin Jacob McCray	8822	2/12/2025	Check Refund		\$962.00 OPERATING
Tori Ann Hudson	8823	2/12/2025	Check Refund		\$4,308.00 OPERATING
Makenna Jenae Berg	8824	2/12/2025	Check Refund		\$3,170.00 OPERATING

Clarendon College**Checks Written****February, 2025**

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Alexander Proctor	8825	2/12/2025	Check Refund	\$307.00	OPERATING
Sophia Marie Bretado	8826	2/12/2025	Check Refund	\$4,242.00	OPERATING
Jeremiah Lamont Deering	8827	2/12/2025	Check Refund	\$684.00	OPERATING
Lacora Brown	8828	2/12/2025	Check Refund	\$6,474.00	OPERATING
Autumn Elizabeth Ash	8829	2/12/2025	Check Refund	\$423.74	OPERATING
Ashley Jordan Land	8830	2/12/2025	Check Refund	\$1,937.00	OPERATING
Wyatt Bradley Oldham	8831	2/12/2025	Check Refund	\$92.50	OPERATING
Noah Hasting Archuleta	8832	2/12/2025	Check Refund	\$2,161.00	OPERATING
Kenzie Mae Harred	8833	2/12/2025	Check Refund	\$1,985.00	OPERATING
April Ruiz Lilly	8834	2/12/2025	Check Refund	\$5,970.00	OPERATING
Koreyan Davis	8835	2/12/2025	Check Refund	\$2,688.00	OPERATING
Denymh Gaige Smith	8836	2/12/2025	Check Refund	\$1,029.00	OPERATING
Clayton Daniel Mosburg	8837	2/12/2025	Check Refund	\$3,464.00	OPERATING
Makynna Rylinn McIntyre	8838	2/12/2025	Check Refund	\$1,428.00	OPERATING
Kennedy Kay Archer	8839	2/12/2025	Check Refund	\$1,193.00	OPERATING
Esta Neema	8840	2/12/2025	Check Refund	\$1,437.00	OPERATING
Esta Neema	8840	2/12/2025	Check Refund	\$163.00	OPERATING
Keeli Cope	8841	2/12/2025	Check Refund	\$2,614.00	OPERATING
Colton G Haywood	8842	2/12/2025	Check Refund	\$5,982.00	OPERATING
Amber Nichole Shull	8843	2/12/2025	Check Refund	\$2,943.39	OPERATING
Jackson Waide Messner	8844	2/12/2025	Check Refund	\$108.00	OPERATING
James Ruff Boivin	8845	2/12/2025	Check Refund	\$1,930.00	OPERATING
Zaylee Shania Rodriguez	8846	2/12/2025	Check Refund	\$1,438.00	OPERATING
Remington Don Roff	8847	2/12/2025	Check Refund	\$3,019.00	OPERATING
Tatum Duane Knight	8848	2/12/2025	Check Refund	\$500.00	OPERATING
Hannah Rene Field	8849	2/12/2025	Check Refund	\$3,070.00	OPERATING
Stephanie Summers	8850	2/12/2025	Check Refund	\$4,517.00	OPERATING
Istzayana Salazar	8851	2/12/2025	Check Refund	\$5,007.00	OPERATING

Clarendon College**Checks Written****February, 2025****Vendor Name**

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Spur James Owens	8852	2/12/2025	Check Refund	\$2,634.00	OPERATING
Tamira Mata	8853	2/12/2025	Check Refund	\$1,970.00	OPERATING
Jake Delwin Houska	8854	2/12/2025	Check Refund	\$60.00	OPERATING
Maria Fernanda Rocha	8855	2/12/2025	Check Refund	\$129.00	OPERATING
Jonathan Blevins	8856	2/12/2025	Check Refund	\$2,853.18	OPERATING
Alexis Morris	8857	2/12/2025	Check Refund	\$302.00	OPERATING
Maddison Gene Putman	8858	2/12/2025	Check Refund	\$497.00	OPERATING
Ashlee Michele Powell	8859	2/12/2025	Check Refund	\$881.56	OPERATING
Berkley Renee Fortier	8860	2/12/2025	Check Refund	\$118.00	OPERATING
Rainy Rose Pilgrim	8861	2/12/2025	Check Refund	\$865.50	OPERATING
Idalis Alessandra Villazana	8862	2/12/2025	Check Refund	\$2,448.00	OPERATING
Alexandria Brean Wilson	8863	2/12/2025	Check Refund	\$897.00	OPERATING
Krystal Angelina Torres	8864	2/12/2025	Check Refund	\$497.00	OPERATING
Jaydee Elyse Foster	8865	2/12/2025	Check Refund	\$1,774.00	OPERATING
Logan Grace Baker	8866	2/12/2025	Check Refund	\$39.39	OPERATING
Zayra Yamile Rodriguez	8867	2/12/2025	Check Refund	\$897.00	OPERATING
Isaac Anthony Denifield	8868	2/12/2025	Check Refund	\$678.00	OPERATING
Gabriel Espinoza	8869	2/12/2025	Check Refund	\$1,422.00	OPERATING
McKinzy Mayleigh Segura	8870	2/12/2025	Check Refund	\$617.00	OPERATING
Taylin Shay Cox	8871	2/12/2025	Check Refund	\$125.00	OPERATING
Mekhi Witter	8872	2/12/2025	Check Refund	\$339.00	OPERATING
Ramon Garcia	8873	2/12/2025	Check Refund	\$796.00	OPERATING
Brynne Voran	8874	2/12/2025	Check Refund	\$897.00	OPERATING
Mandy Lujan	8875	2/12/2025	Check Refund	\$1,922.00	OPERATING
Maggie Autumn Fox	8876	2/12/2025	Check Refund	\$118.00	OPERATING
Quazawn Donta Davis	8877	2/12/2025	Check Refund	\$339.00	OPERATING
Lana Jo Earls	8878	2/12/2025	Check Refund	\$885.00	OPERATING
Devin Joseph Faulkner	8879	2/12/2025	Check Refund	\$678.00	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Trevor Shifflett	8880	2/12/2025	Check Refund	\$65.00	OPERATING
Ethan Riley Luplace	8881	2/12/2025	Check Refund	\$1,822.00	OPERATING
Lylli Marie Kayakone	8882	2/12/2025	Check Refund	\$897.00	OPERATING
Kourtney Lyn Williams	8883	2/12/2025	Check Refund	\$897.00	OPERATING
Paula Lynell Harrison	8884	2/12/2025	Check Refund	\$2,451.00	OPERATING
Antonio Soria	8885	2/12/2025	Check Refund	\$1,969.00	OPERATING
Michelle Guerra	8886	2/12/2025	Check Refund	\$1,199.00	OPERATING
Mollie Allison Crossman	8887	2/12/2025	Check Refund	\$6,230.00	OPERATING
Ashlee Montanna Wortham	8888	2/12/2025	Check Refund	\$1,154.00	OPERATING
Tamra Dawn Christopher	8889	2/12/2025	Check Refund	\$3,227.00	OPERATING
J'Mico A'mon Mitchell	8890	2/12/2025	Check Refund	\$1,672.00	OPERATING
Brian L Osborne	8891	2/12/2025	Check Refund	\$2,972.00	OPERATING
Jocelynn Kaye Thron	8892	2/12/2025	Check Refund	\$6,580.00	OPERATING
Kendell Murream Williams	8893	2/12/2025	Check Refund	\$239.18	OPERATING
Erin LaRue	8894	2/12/2025	Check Refund	\$1,076.00	OPERATING
Erica Leigh Ballinger	8895	2/12/2025	Check Refund	\$3,444.56	OPERATING
Brycen Lynn Epperson	8896	2/12/2025	Check Refund	\$1,409.00	OPERATING
Heiley N Guerra	8897	2/12/2025	Check Refund	\$170.61	OPERATING
Shai Marquis Lira	8898	2/12/2025	Check Refund	\$4,424.88	OPERATING
Yelim America Nunez	8899	2/12/2025	Check Refund	\$2,336.00	OPERATING
Keziah Tiana Dunn	8900	2/12/2025	Check Refund	\$6,472.00	OPERATING
Emily Ragan	8901	2/12/2025	Check Refund	\$785.00	OPERATING
Shianne M Ivy	8902	2/12/2025	Check Refund	\$4,177.00	OPERATING
Keenen Michael Thomason	8903	2/12/2025	Check Refund	\$3,014.00	OPERATING
ACE HARDWARE PAMPA, LLC.	EFT0000000002960	2/12/2025	PAMPA MAINT PARTS	\$3.58	OPERATING
ALLSTATE SECURITY INDUSTRIES, INC.	EFT0000000002961	2/12/2025	CC SECURITY WE 1/27-2/2/2025	\$1,237.50	OPERATING
AquaOne	EFT0000000002962	2/12/2025	1/7/25 CC BOTTLED WATER & DISP	\$49.00	OPERATING
AquaOne	EFT0000000002962	2/12/2025	1/29/25 CC BOTTLED WATER & DIS	\$59.98	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
ASCENDIUM EDUCATION SOLUTIONS	EFT0000000002963	2/12/2025	FAIDE DEBT PREVENTION CONTRAC	\$2,500.00	OPERATING
CANON FINANCIAL SERVICES INC	EFT0000000002964	2/12/2025	FEB 2025 AMARILLO COPIER	\$185.50	OPERATING
CHIEF PLASTIC PIPE & SUPPLY INC.	EFT0000000002965	2/12/2025	PAMPA TOILET REPAIR PARTS	\$29.04	OPERATING
CHIEF PLASTIC PIPE & SUPPLY INC.	EFT0000000002965	2/12/2025	PAMPA PLUMBING PARTS	\$228.34	OPERATING
CHRISTOPHER JAY NAVA	EFT0000000002966	2/12/2025	BB UMPIRE 2/7/2025	\$380.00	OPERATING
CINTAS CORPORATION #491	EFT0000000002967	2/12/2025	JAN 2025 DOUG KIDD UNIFORMS	\$62.52	OPERATING
CINTAS CORPORATION #491	EFT0000000002967	2/12/2025	JAN2025 CC MAINT DEPT UNIFORMS	\$158.52	OPERATING
CINTAS CORPORATION #491	EFT0000000002967	2/12/2025	JAN 2025 TOBY HICKS UNIFORMS	\$41.80	OPERATING
CLARENDON VETERINARY SVC, INC..	EFT0000000002968	2/12/2025	LEC STOCK MEDS & COGGINS TEST	\$370.42	OPERATING
CREATIVE AWARDS & TROPHIES	EFT0000000002969	2/12/2025	2025 CONTEST AWARDS	\$1,580.07	OPERATING
DAVID MOORE	EFT0000000002970	2/12/2025	WB8 OFFICIAL 2/6/2025	\$190.00	OPERATING
DOCUMENT SHREDDING & STORAGE	EFT0000000002971	2/12/2025	JAN 2025 CC SHREDDING	\$124.80	OPERATING
DOCUMENT SHREDDING & STORAGE	EFT0000000002971	2/12/2025	JAN 2025 AMARILLO SHREDDING	\$41.60	OPERATING
DOCUMENT SHREDDING & STORAGE	EFT0000000002971	2/12/2025	JAN 2025 PAMPA SHREDDING	\$83.20	OPERATING
DOCUMENT SHREDDING & STORAGE	EFT0000000002971	2/12/2025	JAN 2025 CHILDRESS SHREDDING	\$41.60	OPERATING
DOUBLE U MARKETING	EFT0000000002972	2/12/2025	FEB25/PAMPA AD AGENT/KOMX/ESL	\$3,379.00	OPERATING
DOUBLE U MARKETING	EFT0000000002972	2/12/2025	FEB25/CLARENDON AD AGENT FEE	\$4,000.00	OPERATING
DOUBLE U MARKETING	EFT0000000002972	2/12/2025	FEB25/AMARILLO AD AGENT FEE	\$1,000.00	OPERATING
DOUBLE U MARKETING	EFT0000000002972	2/12/2025	FEB25/CHILDRESS AD AGENT FEE	\$1,000.00	OPERATING
DYNAVISTICS HOLDINGS, LLC	EFT0000000002973	2/12/2025	JAN 2025 BRIDEY GP CONSULTING	\$5,145.00	OPERATING
GREAT WESTERN DINING SERVICE	EFT0000000002974	2/12/2025	BOARD BILLING WE 2/5/25	\$18,316.13	OPERATING
JEREMY WADE BROWN	EFT0000000002975	2/12/2025	WB8 OFFICIAL 2/6/2025	\$190.00	OPERATING
KEENAN RAMSEY	EFT0000000002976	2/12/2025	BB UMPIRE 2/7/2025	\$380.00	OPERATING
LOWE'S PAY & SAVE INC	EFT0000000002977	2/12/2025	JAN 2025 CC CUSTODIAL SUPPLIES	\$16.99	OPERATING
LOWE'S PAY & SAVE INC	EFT0000000002977	2/12/2025	JAN 2025 CC MAINT SUPPLIES	\$757.47	OPERATING
LOWE'S PAY & SAVE INC	EFT0000000002977	2/12/2025	PARTS FOR LEC BARN DOORS	\$7.30	OPERATING
LOWE'S PAY & SAVE INC	EFT0000000002977	2/12/2025	R.HORSE DRAG PARTS&ANTIFREEZE	\$30.55	OPERATING
LOWE'S PAY & SAVE INC	EFT0000000002977	2/12/2025	JAN 2024 CC AUTO DEPT SUPPLIES	\$64.52	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
LOWE'S PAY & SAVE INC	EFT000000002977	2/12/2025	STU/ACTIVITY POPCORN & OIL	\$44.10	OPERATING
MAX PAYNE JR ABS	EFT000000002978	2/12/2025	FEB2025 FILL RFO NITROGEN TANK	\$65.00	OPERATING
MBS DIRECT	EFT000000002979	2/12/2025	SP-25 F.AIDE STUDENT BOOKS	\$735.82	OPERATING
MBS DIRECT	EFT000000002979	2/12/2025	SP-25 F.AIDE STUDENT BOOKS	\$600.00	OPERATING
NATHAN SULLIVAN	EFT000000002980	2/12/2025	WBB OFFICIAL 2/3/2025	\$190.00	OPERATING
PAMPA ROTARY CLUB	EFT000000002981	2/12/2025	MIKE DAVIS ROTARY DUES	\$70.00	OPERATING
PARS	EFT000000002982	2/12/2025	DEC 2024 PARS SVC FEE	\$300.00	OPERATING
QUILL CORPORATION #2169750	EFT000000002983	2/12/2025	HOLLY IRISH PRINT CARTRIDGE	\$196.87	OPERATING
QUILL CORPORATION #2169750	EFT000000002983	2/12/2025	JULISSA PRINTER CARTRIDGE	\$76.99	OPERATING
QUILL CORPORATION #2169750	EFT000000002983	2/12/2025	STU-SVC 3 NEW OFFICE CHAIRS	\$563.25	OPERATING
QUILL CORPORATION #2169750	EFT000000002983	2/12/2025	JANEAN OFFICE SUPPLIES	\$58.57	OPERATING
RUN BUSINESS SOLUTIONS	EFT000000002984	2/12/2025	3 MONITORS/STU-SVC DEPT.	\$633.03	OPERATING
TIMOTHY LEE EVINS	EFT000000002985	2/12/2025	WBB OFFICIAL 2/6/2025	\$190.00	OPERATING
YourNewSchool	EFT000000002986	2/12/2025	SP-2025 AMARILLO COSMO KITS	\$14,330.50	OPERATING
YourNewSchool	EFT000000002986	2/12/2025	SP-2025 PAMPA COSMO KITS	\$2,891.28	OPERATING
YourNewSchool	EFT000000002986	2/12/2025	SP-2025 CHILDRESS COSMO KITS	\$2,235.20	OPERATING
HERRING NATIONAL BANK	STOPPMT #7390 #5128	2/12/2025	STOP PMT CK#5128	\$15.00	OPERATING
HERRING NATIONAL BANK	STOPPMT #7390 #5128	2/12/2025	STOP PMT CK#7390	\$15.00	OPERATING
VISA	C.RUSSELL 2/14/25	2/14/2025	BB TEAM MEAL@MELISSA TX	\$258.56	OPERATING
VISA	DRIVER#1 2/14/25	2/14/2025	R.HORSE @FT.WORTH 2/4-7	\$544.50	OPERATING
VISA	DRIVER#2 2/14/2025	2/14/2025	ENGRAVING MEATS TEAM TROPHYS	\$108.91	OPERATING
VISA	L.ALEXANDER 2/14/25	2/14/2025	SB GAME CHANGER ANNUAL FEES	\$97.41	OPERATING
VISA	L.ALEXANDER 2/14/25	2/14/2025	SB MEAL @VERNON 2/5/25	\$167.42	OPERATING
VISA	L.ALEXANDER 2/14/25	2/14/2025	SB@CISCO 2/7-8 HOTEL/MEALS	\$1,319.16	OPERATING
VISA	L.ALEXANDER 2/14/25	2/14/2025	SB MEALS@WACO	\$604.76	OPERATING
VISA	L.ALEXANDER 2/14/25	2/14/2025	SB MED KIT SUPPLIES	\$51.94	OPERATING
VISA	PAMPA 2/14/2025	2/14/2025	PAMPA MAINT VEHICLE FUEL	\$50.25	OPERATING
VISA	PAMPA 2/14/2025	2/14/2025	CPR CLASS@CHILDRESS 1/23/25	\$64.00	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
VISA	PAMPA 2/14/2025	2/14/2025	CPR CLASS@PAMPA 2/3/25	\$72.00	OPERATING
VISA	PAMPA 2/14/2025	2/14/2025	CPR CLASS@PAMPA 1/29/25	\$48.00	OPERATING
VISA	PAMPA 2/14/2025	2/14/2025	PAMPA ROACH RUN FUEL	\$19.63	OPERATING
VISA	PAMPA 2/14/2025	2/14/2025	CPR CLASS@PAMPA 1/30/25	\$16.00	OPERATING
VISA	PAMPA 2/14/2025	2/14/2025	CPR CLASS@PAMPA 1/23/25	\$48.00	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	SB BATS & WATER JUGS	\$1,709.82	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	CC CUSTODIAL SUPPLIES	\$412.01	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	GOOGLE DOORBELL & CAMERA	\$393.99	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	FEB25/AMAZON PRIME MEMBERSHIP	\$14.99	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	SUPPLIES FOR STU/ACT SMORES	\$169.89	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	WILL/HUNTER ROOMS@DALLAS	\$1,016.62	OPERATING
VISA	VISA#1 2/14/2025	2/14/2025	RFO THANK YOUS & POST CARDS	\$300.14	OPERATING
VISA	VISA#4 2/14/2025	2/14/2025	HUNTER/WILL FUEL/MEAL@DALLAS	\$155.87	OPERATING
VISA	VISA#4 2/14/2025	2/14/2025	SP-25 AMA COSMO STU PERMITS	\$400.00	OPERATING
VISA	VISA#4 2/14/2025	2/14/2025	SP-25 CHILDR COSMO STU PERMITS	\$75.00	OPERATING
VISA	VISA#4 2/14/2025	2/14/2025	CAF PROOFING CABINET SWITCH	\$73.04	OPERATING
VISA	VISA#4 2/14/2025	2/14/2025	SP-25 AMA COSMO STU.PERMIT	\$25.00	OPERATING
VISA	J.TREICHEL 2/17/25	2/17/2025	JUDGING HOTEL@SAN ANTONIO	\$798.72	OPERATING
ARMSTRONG MCCALL BEAUTY SUPPLY	8904	2/19/2025	AMARILLO COSMO SUPPLIES	\$13.07	OPERATING
ABRAHAM VILLEGAS	8905	2/19/2025	WBB OFFICIAL 2/13/2025	\$190.00	OPERATING
BRADY HOFFMAN	8906	2/19/2025	DROVE MEATS PRACTICE 2/14/25	\$120.00	OPERATING
BRADY HOFFMAN	8906	2/19/2025	DROVE MEATS PRACTICE 2/7-8/25	\$100.00	OPERATING
CIRCLE N APPLIANCE	8907	2/19/2025	SHIPPING DORM WASHER/DRYER	\$180.00	OPERATING
CORY B. RUSSELL	8908	2/19/2025	REIMB B8 TEAM MEAL	\$243.51	OPERATING
HOLLY IRISH	8909	2/19/2025	R.HORSE STALL SIGN DEPOSIT	\$657.19	OPERATING
NRG BUSINESS	8910	2/19/2025	JAN 2025 CHILDRESS ELECTRIC	\$1,420.30	OPERATING
O'REILLY AUTO PARTS	8911	2/19/2025	CDL SEMI'S DEICER	\$3.99	OPERATING
O'REILLY AUTO PARTS	8911	2/19/2025	CDL SEMI WIPER BLADES/ANTI GEL	\$259.86	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
PEARSON EDUCATION, INC.	8912	2/19/2025	SP-2025 MATH XL CODES	\$20,997.00	OPERATING
SARA BEAN	8913	2/19/2025	DROVE MEATS PRACTICE 2/8-9/25	\$100.00	OPERATING
SARA BEAN	8913	2/19/2025	DROVE MEATS PRACTICE 2/14/25	\$120.00	OPERATING
BIG INNING, INC.	8914	2/19/2025	SB UNIFORM TOPS	\$4,550.00	OPERATING
SCOTT L. CAMPBELL	8915	2/19/2025	MBB/WBB GYM SECURITY 2/13/25	\$200.00	OPERATING
SOUTHWESTERN ELECTRIC POWER	8916	2/19/2025	FEB25/CC STREET LIGHTS	\$302.47	OPERATING
SOUTHWESTERN ELECTRIC POWER	8916	2/19/2025	FEB 2025 CC CAMPUS ELECTRIC	\$10,473.28	OPERATING
WINSUPPLY OF AMARILLO	8917	2/19/2025	CAFETERIA HOT WATER HEATER	\$5,851.32	OPERATING
XCEL ENERGY	8918	2/19/2025	JAN 2025 AMARILLO ELECTRIC	\$528.05	OPERATING
ALLSTATE SECURITY INDUSTRIES, INC.	EFT000000002987	2/19/2025	CC SECURITY 2/3-2/9/2025	\$1,237.50	OPERATING
AMA TECHTEL COMMUNICATIONS	EFT000000002988	2/19/2025	FEB 2025 CC T-1 LINE	\$1,919.32	OPERATING
AMA TECHTEL COMMUNICATIONS	EFT000000002988	2/19/2025	FEB 2025 AMARILLO PHONE	\$187.41	OPERATING
AMA TECHTEL COMMUNICATIONS	EFT000000002988	2/19/2025	FEB25 CC T-1 LINE	\$460.00	OPERATING
ATMOS ENERGY 3052368050	EFT000000002989	2/19/2025	JAN 2025 CHILDRESS GAS	\$2,001.64	OPERATING
B & J WELDING SUPPLY	EFT000000002990	2/19/2025	WELDER FOR RODEO DEPARTMENT	\$5,593.50	OPERATING
BARRETT & CROFOOT FEEDYARDS	EFT000000002991	2/19/2025	FEEDING JUDGING CONTEST STOCK	\$110.18	OPERATING
BARRETT & CROFOOT FEEDYARDS	EFT000000002991	2/19/2025	PURCHASE 24 CONTEST STEERS	\$66,535.14	OPERATING
BART CRAIG	EFT000000002992	2/19/2025	WBB OFFICIAL 2/13/2025	\$190.00	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 STU SVC'S COPIER	\$120.58	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 PAMPA COPIER	\$136.21	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 CC ADMIN COPIER	\$172.21	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 NURSING COPIER	\$120.58	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 CHILDRESS COPIER	\$120.58	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 BAC COPIER	\$110.62	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 LIBRARY COPIER	\$136.68	OPERATING
CANON FINANCIAL SERVICES INC	EFT000000002993	2/19/2025	FEB 2025 RFO COPIER	\$120.58	OPERATING
CHIEF PLASTIC PIPE & SUPPLY INC.	EFT000000002994	2/19/2025	PLUMBING PARTS @PAMPA CTR	\$455.11	OPERATING
CHILL OUT HEAT & A/C	EFT000000002995	2/19/2025	REPAIR HEATER/CC ADM CONF ROOM	\$1,120.53	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
CREATIVE AWARDS & TROPHIES	EFT000000002996	2/19/2025	ROSETTE'S FOR JUDGING CONTEST	\$1,567.50	OPERATING
DEBBIE LIN ROBERTS	EFT000000002997	2/19/2025	SB UMPIRE 2/10/2025	\$540.00	OPERATING
DEBBIE LIN ROBERTS	EFT000000002997	2/19/2025	SB UMPIRE 2/17/2025	\$540.00	OPERATING
DECEE SURRATT	EFT000000002998	2/19/2025	REIMB INSTR BREAKFAST/MEETING	\$65.98	OPERATING
FRED LEIGHTON	EFT000000002999	2/19/2025	SB UMPIRE 2/10/2025	\$360.00	OPERATING
GREAT WESTERN DINING SERVICE	EFT000000003000	2/19/2025	BOARD BILLING WE 2/12/2025	\$18,237.52	OPERATING
JIMMY GAUNA	EFT000000003001	2/19/2025	SB UMPIRE 2/17/2025	\$540.00	OPERATING
JIMMY GAUNA	EFT000000003001	2/19/2025	SB UMPIRE 2/11/2025	\$180.00	OPERATING
MORRIS GLASS OF THE TX PANHANDLE, LLC	EFT000000003002	2/19/2025	GYM WINDOW/BROKE BY MBB PLAYER	\$300.00	OPERATING
TIMOTHY LEE EVINS	EFT000000003003	2/19/2025	WBB OFFICIAL 2/13/2025	\$190.00	OPERATING
UNIFIRST HOLDINGS ACCT#0898/0896	EFT000000003004	2/19/2025	FEB25/PAMPA CUSTODIAL SUPPLIES	\$184.49	OPERATING
UNIFIRST HOLDINGS ACCT#0898/0896	EFT000000003004	2/19/2025	FEB25/PAMPA COSMO SUPPLIES	\$190.19	OPERATING
VISA	B.COCHRAN 2/20/25	2/20/2025	MBB MEAL 2/6/2025	\$95.00	OPERATING
VISA	B.COCHRAN 2/20/25	2/20/2025	MBB MEALS@LEVELLAND 2/17	\$329.53	OPERATING
VISA	B.COCHRAN 2/20/25	2/20/2025	MBB MEALS 2/13/2025	\$95.00	OPERATING
VISA	B.FRANKS 2/20/2025	2/20/2025	BRET/2 RECRUITS & FAMILY MEALS	\$112.39	OPERATING
VISA	C.RUSSELL 2/20/2025	2/20/2025	BB@CISCO 2/14-15	\$2,000.53	OPERATING
VISA	C.UPTON 2/20/2025	2/20/2025	2 CDL STUDENT EXAMS	\$82.00	OPERATING
VISA	DRIVER#1 2/20/25	2/20/2025	R.HORSE AIRBNB@FT WORTH	\$836.98	OPERATING
VISA	M.JAMES 2/20/2025	2/20/2025	WBB MEAL 2/6/2025	\$63.00	OPERATING
VISA	M.JAMES 2/20/2025	2/20/2025	FITNESS CENTER TREADMILLS	\$1,296.84	OPERATING
VISA	M.JAMES 2/20/2025	2/20/2025	WBB MEAL 2/13/2025	\$63.00	OPERATING
VISA	M.JAMES 2/20/2025	2/20/2025	TRAP BARS FOR FITNESS CENTER	\$368.02	OPERATING
VISA	T.BUCKHAULTS 2/20/25	2/20/2025	TEX/SACSCOC MEAL W/DR.YOUNG	\$37.44	OPERATING
VISA	VISA#1 2/20/2025	2/20/2025	FEB 2025 STARLINK SUBSCRIPTION	\$560.00	OPERATING
VISA	VISA#1 2/20/2025	2/20/2025	DR.YOUNG/SACSCOC VISIT 2/11-12	\$326.96	OPERATING
VISA	VISA#1 2/20/2025	2/20/2025	STU ACTIVITY HERSHEY BARS	\$55.90	OPERATING
VISA	VISA#4 2/20/2025	2/20/2025	PIZZA/STUDENTS@LEVELLAND GAMES	\$210.19	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
VISA	W.SMITH 2/20/2025	2/20/2025	WYATT/FUEL TO HAUL SP-25 STOCK	\$170.37	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	FUEL/STUDENTS/LEVELLAND GAMES	\$146.82	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	FEB 2025 MEATS/L STOCK FUEL	\$1,556.78	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	FEB 2025 BB TRAVEL FUEL	\$588.28	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	VB FUEL/PLAYER TO DR.APPTS	\$31.62	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	FEB 2025 SB TRAVEL FUEL	\$758.15	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	FEB 2025 MBB TRAVEL FUEL	\$24.48	OPERATING
U.S. BANK VOYAGER	FEB 2025 FLEET FUEL	2/25/2025	FEB 2024 RFO TRAVEL FUEL	\$131.22	OPERATING
VISA	L.ALEXANDER 2/25/25	2/25/2025	SB HOTEL@MIDLAND 5/1-2	\$1,422.06	OPERATING
Kensie Drew Kimball	8919	2/26/2025	Check Refund	\$866.00	OPERATING
Jodee Wayne Pigg	8920	2/26/2025	Check Refund	\$1,250.00	OPERATING
Yanci Deene Hutchison	8921	2/26/2025	Check Refund	\$1,086.00	OPERATING
Aspen Brett Miller	8922	2/26/2025	Check Refund	\$1,000.00	OPERATING
Angelina Alcozer	8923	2/26/2025	Check Refund	\$1,283.00	OPERATING
Angelina Alcozer	8923	2/26/2025	Check Refund	\$2,500.00	OPERATING
Clarissa Lisette Lepe	8924	2/26/2025	Check Refund	\$437.00	OPERATING
Analysa Rios	8925	2/26/2025	Check Refund	\$514.00	OPERATING
Brighton Alan Wooton	8926	2/26/2025	Check Refund	\$250.00	OPERATING
Rye McCall Reynolds	8927	2/26/2025	Check Refund	\$1,500.00	OPERATING
Ellie Grace Cameron	8928	2/26/2025	Check Refund	\$218.00	OPERATING
Neicha Marie Marsaw	8929	2/26/2025	Check Refund	\$1,021.00	OPERATING
Leah Nicole Becerra	8930	2/26/2025	Check Refund	\$1,380.00	OPERATING
Paula Bernardo Carvalho	8931	2/26/2025	Check Refund	\$1,293.00	OPERATING
Nikolas Coronado	8932	2/26/2025	Check Refund	\$659.00	OPERATING
Nikita Munguia	8933	2/26/2025	Check Refund	\$2,172.00	OPERATING
Grant Haynes	8934	2/26/2025	Check Refund	\$42.65	OPERATING
Haylie Anisa Enriquez	8935	2/26/2025	Check Refund	\$866.00	OPERATING
Addison Blair Butler	8936	2/26/2025	Check Refund	\$85.30	OPERATING

Clarendon College**Checks Written****February, 2025**

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Ketreonna Laneshia Branch	8937	2/26/2025	Check Refund	\$1,346.00	OPERATING
Paris Chanler Lamb	8938	2/26/2025	Check Refund	\$497.00	OPERATING
Carter Martin Munson	8939	2/26/2025	Check Refund	\$225.00	OPERATING
Mitchell Dewayne Pace	8940	2/26/2025	Check Refund	\$1,500.00	OPERATING
Aaron Senties	8941	2/26/2025	Check Refund	\$1,821.00	OPERATING
Railey Chase Nieto	8942	2/26/2025	Check Refund	\$250.00	OPERATING
Christian Jousha Don Lemons	8943	2/26/2025	Check Refund	\$134.25	OPERATING
Keeli Cope	8944	2/26/2025	Check Refund	\$2,529.00	OPERATING
Shannon Eileen Hanen	8945	2/26/2025	Check Refund	\$1,415.00	OPERATING
Harmony Lain Lane	8946	2/26/2025	Check Refund	\$119.43	OPERATING
Brynne Voran	8947	2/26/2025	Check Refund	\$4,701.00	OPERATING
Chance Britten	8948	2/26/2025	Check Refund	\$452.00	OPERATING
Antonio Soria	8949	2/26/2025	Check Refund	\$1,732.00	OPERATING
Mayra Salazar	8950	2/26/2025	Check Refund	\$1,628.50	OPERATING
ARMSTRONG MCCALL BEAUTY SUPPLY	8951	2/26/2025	AMARILLO COSMO SUPPLIES	\$55.20	OPERATING
ARMSTRONG MCCALL BEAUTY SUPPLY	8951	2/26/2025	PAMPA COSMO COLOR SUPPLIES	\$1,944.10	OPERATING
ABBY MIXON PERFORMANCE HORSE	8952	2/26/2025	RANCH HORSE CLINIC 3/12-13	\$2,400.00	OPERATING
AMARILLO FIRE & SAFETY, INC.	8953	2/26/2025	AMARILLO ANNUAL FIRE INSPECT	\$91.00	OPERATING
BRANDON PORTER, JR.	8954	2/26/2025	WBB OFFICIAL 2/20/2025	\$190.00	OPERATING
BRET FRANKS	8955	2/26/2025	M.RODEO TRAVEL \$ /SWEETWATER	\$700.00	OPERATING
CAROLINA BIOLOGICAL SUPPLY CO.	8956	2/26/2025	CHILDR & CC BIOLOGY LAB SUPP.	\$1,380.83	OPERATING
CHILDRESS CO. 4-H	8957	2/26/2025	CHILDRESS RODEO BANNER AD	\$60.00	OPERATING
CITY OF AMARILLO	8958	2/26/2025	MAR 2025 AMARILLO PARKING LOT	\$200.00	OPERATING
CLARENDON CHAMBER OF COMMERCE	8959	2/26/2025	2025 BANQ.TABLE/YOUTH AWA/DUES	\$850.00	OPERATING
CORY B. RUSSELL	8960	2/26/2025	REIMB 2 BB TEAM MEALS	\$553.31	OPERATING
EDWARD JONES	8961	2/26/2025	OPERATING INVEST PER FIN.COMMI	\$250,000.00	OPERATING
ELLIOTT ELECTRIC SUPPLY, INC.	8962	2/26/2025	LED BULBS PAMPA CENTER	\$262.50	OPERATING
EAN SERVICES, LLC	8963	2/26/2025	TEX TOLLS TO/FROM SACS CONF.	\$23.50	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
GALE/CENGAGE LEARNING	8964	2/26/2025	GALE E-BOOK HOSTING FEE	\$150.00	OPERATING
LOTT HOME CENTER	8965	2/26/2025	CHILDRESS COSMO PLUMB PARTS	\$13.56	OPERATING
MCGRAW-HILL LLC	8966	2/26/2025	SPRING 2025 SPANISH CODES	\$1,838.25	OPERATING
MICHAEL W. TIMMINS JR	8967	2/26/2025	WBB OFFICIAL 2/20/2025	\$190.00	OPERATING
NORTH TEXAS TOLLWAY AUTHORITY	8968	2/26/2025	WILL/HUNTER TOLLS@DALLAS 2/2	\$5.70	OPERATING
RDA PROMART AMARILLO	8969	2/26/2025	AMA COSMO HAIR COLOR	\$47.90	OPERATING
SCOTT L. CAMPBELL	8970	2/26/2025	MBB/WBB GAME SECURITY 2/20/25	\$200.00	OPERATING
THESIS AMERICA, INC.	8971	2/26/2025	CAMS ANNUAL MAINT & LICENSE	\$81,378.47	OPERATING
VEXUS FIBER	8972	2/26/2025	JAN/FEB PAMPA FIBER OPTIC	\$1,610.00	OPERATING
LINDE GAS & EQUIPMENT, INC	8973	2/26/2025	PAMPA & CC WELDING BOTTLE RENT	\$354.11	OPERATING
LINDE GAS & EQUIPMENT, INC	8973	2/26/2025	PAMPA & CC WELDING SUPPLIES	\$1,583.39	OPERATING
WYATT SMITH	8974	2/26/2025	W.RODEO TRAVEL \$/SWEETWATER	\$500.00	OPERATING
X CROSS X. LTD	8975	2/26/2025	LEC/2 BUNDLES BERMUDA GRASS	\$420.00	OPERATING
YELLOW CITY PEST CONTROL	8976	2/26/2025	FEB 2025 CC PEST CONTROL	\$372.99	OPERATING
YELLOW CITY PEST CONTROL	8976	2/26/2025	FEB25 CHILDRESS BUG SPRAYING	\$157.99	OPERATING
YELLOW CITY PEST CONTROL	8976	2/26/2025	FEB 2025 AMARILLO BUG SPRAY	\$82.99	OPERATING
YELLOW CITY PEST CONTROL	8976	2/26/2025	FEB 2025 PAMPA BUG SPRAYING	\$127.99	OPERATING
287 AG, LLC.	EFT0000000003005	2/26/2025	RODEO STOCK FEED	\$1,014.00	OPERATING
ACE HARDWARE PAMPA, LLC.	EFT0000000003006	2/26/2025	PAMPA MAINT DEPT SUPPLIES	\$31.96	OPERATING
ACE HARDWARE PAMPA, LLC.	EFT0000000003006	2/26/2025	PAMPA MAINT TOOLS FOR DRYWALL	\$42.55	OPERATING
ALLSTATE SECURITY INDUSTRIES, INC.	EFT0000000003007	2/26/2025	CC CAMPUS SECURITY 2/10-16/25	\$1,237.50	OPERATING
AMA TECHTEL COMMUNICATIONS	EFT0000000003008	2/26/2025	SP-2025 STUDENT WIFI ACCESS	\$6,150.00	OPERATING
ATMOS ENERGY 3045565154	EFT0000000003009	2/26/2025	FEB 2025 PAMPA CAMPUS GAS	\$655.36	OPERATING
ATMOS ENERGY 3045565154	EFT0000000003009	2/26/2025	FEB 2025 AMARILLO GAS	\$394.00	OPERATING
BARTLETT'S LUMBER & HARDWARE	EFT0000000003010	2/26/2025	PAMPA INDUST/MAINT SUPPLIES	\$76.85	OPERATING
BURMAX	EFT0000000003011	2/26/2025	PAMPA COSMO SUPPLIES	\$3,369.14	OPERATING
SPARKLIGHT#104869755	EFT0000000003012	2/26/2025	FEB 2025 PAMPA CABLE/WIFI	\$977.00	OPERATING
CITY OF PAMPA 495/499/545/546	EFT0000000003013	2/26/2025	FEB 2025 PAMPA WATER	\$531.98	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
DEBBIE LIN ROBERTS	EFT000000003014	2/26/2025	SB UMPIRE 2ND GAME 2/11/2025	\$180.00	OPERATING
EAN SERVICES, LLC	EFT000000003015	2/26/2025	FEB 2025 TEX LEASE CAR	\$923.12	OPERATING
EAN SERVICES, LLC	EFT000000003015	2/26/2025	FEB 2025 FLEET VEHICLE LEASE	\$923.12	OPERATING
GREAT WESTERN DINING SERVICE	EFT000000003016	2/26/2025	BOARD BILLING WE 2/19/25	\$18,158.91	OPERATING
GREAT WESTERN DINING SERVICE	EFT000000003016	2/26/2025	LUNCH SACSCOC REP & CC EMPLOY.	\$56.00	OPERATING
HANK PAYMENTS CORP.	EFT000000003017	2/26/2025	DEC 2024 HANK PAYMENTS FEE	\$137.75	OPERATING
HANK PAYMENTS CORP.	EFT000000003017	2/26/2025	NOV 2024 HANK PAYMENTS FEE	\$153.25	OPERATING
JIMMY GAUNA	EFT000000003018	2/26/2025	SB UMPIRE 2/11/25 2ND GAME	\$180.00	OPERATING
MUSTARD BASKET CO.	EFT000000003019	2/26/2025	MAR 2025 WEB SUPPORT	\$2,630.00	OPERATING
NATHAN SULLIVAN	EFT000000003020	2/26/2025	WBB OFFICIAL 2/20/2025	\$190.00	OPERATING
RUN BUSINESS SOLUTIONS	EFT000000003021	2/26/2025	MAR 2025 COMPUTER FEES	\$19,857.56	OPERATING
RUN BUSINESS SOLUTIONS	EFT000000003021	2/26/2025	KAREN PRINTER	\$999.99	OPERATING
RUN BUSINESS SOLUTIONS	EFT000000003021	2/26/2025	LIBRARY COUNTER PRINTER	\$817.50	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 STU SVC'S COPIER	\$114.04	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 BAC COPIER	\$9.00	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 LIBRARY COPIER	\$15.00	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 PAMPA COPIER	\$104.48	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 NURSING COPIER	\$164.23	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 RFO COPIER	\$118.75	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 CHILDRESS COPIER	\$78.77	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/26/2025	2/10-3/9/25 CC ADMIN COPIER	\$40.83	OPERATING
TASCOSA OFFICE MACHINES	EFT000000003022	2/28/2025	2/28/2025 AFLAC	\$19.60	OPERATING
AFLAC	8977	2/28/2025	2/14/2025 AFLAC	\$19.60	OPERATING
LIBERTY NATIONAL LIFE INSURANCE	8979	2/28/2025	2/28/25 LIBERTY NATIONAL	\$256.11	OPERATING
LIBERTY NATIONAL LIFE INSURANCE	8979	2/28/2025	LIB.NATIONAL 2/14/25	\$389.76	OPERATING
LIBERTY NATIONAL LIFE INSURANCE	8979	2/28/2025	LIB NATIONAL 2/28/25	\$389.61	OPERATING
LIBERTY NATIONAL LIFE INSURANCE	8979	2/28/2025	2/14/25 LIBERTY NATIONAL	\$256.11	OPERATING
MFS SERVICE CENTER, INC.	8980	2/28/2025	MFS 2/14/25	\$25.00	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
MFS SERVICE CENTER, INC.	8980	2/28/2025	2/28/25 MFS	\$25.00	OPERATING
NEW YORK LIFE INSURANCE CO	8981	2/28/2025	2/14/2025 NEW YORK LIFE	\$194.69	OPERATING
NEW YORK LIFE INSURANCE CO	8981	2/28/2025	NEW YORK LIFE 2/28/25	\$194.69	OPERATING
OFFICE OF ATTORNEY GEN. TX STATE DISBURSEMENT UNIT	8982	2/28/2025	CHILD SUPP 2/4/2025	\$728.00	OPERATING
OFFICE OF ATTORNEY GEN. TX STATE DISBURSEMENT UNIT	8982	2/28/2025	2/28/25 CHILD SUPPORT	\$728.00	OPERATING
OFFICE OF ATTORNEY GENERAL	8983	2/28/2025	CHILD SUPP 2/14/25	\$150.00	OPERATING
OFFICE OF ATTORNEY GENERAL	8983	2/28/2025	CHILD SUPPORT 2/28/25	\$150.00	OPERATING
OFFICE OF ATTORNEY GENERAL	8983	2/28/2025	2/28/25 CHILD SUPPORT	\$147.50	OPERATING
OFFICE OF ATTORNEY GENERAL	8983	2/28/2025	2/14/2025 CHILD SUPPORT	\$147.50	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 TENORIO VALIC	\$70.93	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 CHANEY VALIC	\$77.78	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/28/25 MINOTTO VALIC	\$80.91	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	ZORNES 2/28/25	\$44.00	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	JOHNSON 2/28/25	\$80.30	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 JOHNSON VALIC	\$80.91	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/28/25 COCHRAN VALIC	\$123.30	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	TENORIO 2/28/25	\$70.40	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/28/25 JOHNSON VALIC	\$80.91	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 MINOTTO/VALIC	\$80.30	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	ZORNES VALIC 2/14/25	\$44.00	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	CHANEY 2/14/25 VALIC	\$77.00	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	MINOTTO 2/28/25	\$80.30	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	COCHRAN 2/28/25	\$122.38	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/28/25 ZORNES VALIC	\$44.33	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 COCHRAN VALIC	\$123.30	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	COCHRAN VALIC 2/14/25	\$122.38	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	JOHNSON 2/14/25 VALIC	\$80.30	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/28/25 TENORIO VALIC	\$70.93	OPERATING

Clarendon College

Checks Written

February, 2025

Vendor Name	Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/28/25 CHANEY VALIC	\$77.38	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	CHANEY 2/28/25	\$77.00	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	TENORIO VALIC 2/14/25	\$70.40	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 ZORNES VALIC	\$44.33	OPERATING
VALIC C/O JP MORGAN CHASE	8984	2/28/2025	2/14/25 VALIC/MINOTTO	\$80.91	OPERATING
VISA	C.RUSSELL 2/28/25	2/28/2025	BB HOTEL @DALLAS 2/21-22	\$1,468.00	OPERATING
VISA	C.RUSSELL 2/28/25	2/28/2025	BB RADAR GUN REPAIR	\$217.50	OPERATING
VISA	C.RUSSELL 2/28/25	2/28/2025	BB LAS VEGAN NM HOTEL DEPOSIT	\$414.11	OPERATING
VISA	D.MARMOLEJO 2/28/25	2/28/2025	WBB MEAL @ODESSA	\$150.88	OPERATING
VISA	D.MARMOLEJO 2/28/25	2/28/2025	WBB MEAL 2/20/2025	\$63.00	OPERATING
VISA	DRIVER#2 2/28/25	2/28/2025	LSTOCK HOTEL/MEAL@SAN ANTONIO	\$814.57	OPERATING
PRINCIPAL DENTAL # 1162253-10001	FEB25/DENTAL PREMIUM	2/28/2025	2/14/2025 PRINCIPAL DENTAL	\$225.45	OPERATING
PRINCIPAL DENTAL # 1162253-10001	FEB25/DENTAL PREMIUM	2/28/2025	2/28/2025 PRINCIPAL DENTAL	\$225.36	OPERATING
VISA	J.TREICHEL 2/28/25	2/28/2025	NACTA MEMBERSHIP DUES	\$100.00	OPERATING
VISA	J.TREICHEL 2/28/25	2/28/2025	LSTOCK@SAN ANTONIO HOTEL/MEAL	\$1,123.19	OPERATING
VISA	M.JAMES 2/28/25	2/28/2025	AED FOR GYM/BB-SB FIELDS	\$3,198.00	OPERATING
VISA	PAMPA 2/28/25	2/28/2025	MIKE/STUDENTS MEAL@PAMPA	\$65.24	OPERATING
VISA	PAMPA 2/28/25	2/28/2025	PAMPA WELDING MAINT TOOL	\$39.99	OPERATING
VISA	PAMPA 2/28/25	2/28/2025	PAMPA WELDING PROPANE	\$72.45	OPERATING
VISA	T.BUCKHAULTS 2/28/25	2/28/2025	TEX/MICHAEL FLIGHTS/ATLANTA	\$767.58	OPERATING
CLARENDON COLLEGE	7 DD STU REFUND RET	2/18/2025	7 DD STUDENT REFUND RETURNS	\$28,409.46	DISBURSEMENT
ERS	JAN25/ERS-HSA TEXNET	2/3/2025	JAN 2025 ERS/HSA TEXNET	\$190.00	PAYROLL
PARS/ACH	JAN 2025 PARS PMT	2/5/2025	JAN 2025 PARS PMT	\$2,389.93	PAYROLL
Teacher Retirement System	JAN 2025 TRS TEXNET	2/5/2025	JAN 2025 TRS TEXNET	\$59,475.10	PAYROLL
Teacher Retirement System	JAN25/TRS-ER ADJUST	2/5/2025	JAN 2025 TRS ER ADJUSTMENT	\$198.00	PAYROLL
ERS	JAN25/ERS TEXNET	2/12/2025	JAN 2025 ERS TEXNET	\$86,977.52	PAYROLL
IRS/PMT	IRS 2/14/2025 FT,PT	2/14/2025	IRS 2/14/2025 FT,PT	\$19,449.23	PAYROLL
IRS/PMT	IRS 2/28/2025 FT,PT	2/26/2025	IRS 2/28/2025 FT,PT	\$19,639.50	PAYROLL

Clarendon College
Checks Written
February, 2025
Vendor Name

Payment Number	Payment Date	Transaction Description	Applied Amount	Checkbook ID
Totals			\$1,519,592.07	

CLARENDON COLLEGE BOARD OF REGENTS MONTHLY INVESTMENT REPORT

2/28/2025

Feb-25

Fund	Type	Purchase Date	Maturity Date	Yield	Market Value		Income	Maturity	Withdrawals	Additions	Expenses	Accrued Interest	Appreciation (Depreciation)	Market Value 2/28/2025
					09/01/2024	1/31/2025								
216-21515-1-4	Edward Jones	12/28/2020			\$ 2,141,373.37	\$ 2,204,978.12	\$ 5,774.83	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 2,210,752.95
Endow Restricted 216-21515-1-4	Edward Jones	2/11/2021			\$ 1,140,727.08	\$ 1,174,679.62	\$ 4,209.82	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 1,178,889.44
Endow Unrestricted 216-21784-1-8	Edward Jones	11/17/2023			\$ 2,067,943.01	\$ 2,615,615.98	\$ 9,378.89	\$ -	\$ -	\$ 250,000.00	\$ -	\$ -	\$ -	\$ 2,874,994.87
Operating Account 216-24353	Edward Jones	3/27/2023			\$ 240,954.85	\$ 245,768.28	\$ 881.25	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 246,649.53
Agency Account 216-23649-1-9	Edward Jones	4/14/2022		1.50%	\$ 2,187.48	\$ 2,201.36	\$ 2.53	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 2,203.89
Investment Account 70173087	Herring Bank			4.4888%		\$ 1,011,534.12	\$ 3,953.40			\$ 750,000.00				\$ 1,765,487.52
Operating Account TX-01-1207-0001	Texas Class	11/1/2024												
					\$ 5,593,185.79	\$ 7,254,777.48	\$ 24,200.72	\$ -	\$ -	\$ 1,000,000.00	\$ -	\$ -	\$ -	\$ 8,278,978.20

Summary

	Market Value		Income - Expense
	1/31/2025	2/28/2025	
		Growth	
216-21515-1-4	\$ 2,204,978.12	\$ 2,210,752.95	\$ 5,774.83
216-21784-1-8	\$ 1,174,679.62	\$ 1,178,889.44	\$ 4,209.82
216-24353-1-3	\$ 2,615,615.98	\$ 2,874,994.87	\$ 259,378.89
216-23649-1-9	\$ 245,768.28	\$ 246,649.53	\$ 881.25
70173087	\$ 2,201.36	\$ 2,203.89	\$ 2.53
TX-01-1207-0001	\$ 1,011,534.12	\$ 1,765,487.52	\$ 753,953.40
	\$ 7,254,777.48	\$ 8,278,978.20	\$ 1,024,200.72

Insured Bank Deposit

Edward Jones Insured Bank Deposit Account 216-21515-1-4	1.55%	\$229.28
Edward Jones Insured Bank Deposit Account 216-21784-1-8	1.55%	\$943.57
Edward Jones Insured Bank Deposit Account 216-24353-1-3	1.55%	\$250,000.18
Edward Jones Insured Bank Deposit Account 216-23649-1-9	1.55%	\$1.53

Money Market

PIMCO Government Money Market A - Account 216-21515-1-4	3.97%	\$2,210,523.67
PIMCO Government Money Market A - Account 216-21784-1-8	3.84%	\$1,177,945.87
PIMCO Government Money Market A - Account 216-24353-1-3	4.57%	\$2,624,994.69
PIMCO Government Money Market A - Account 216-23649-1-9	4.75%	\$246,648.00

Donley Appraisal District

HISTORY SUMMARY BY JURISDICTION Posted years

From 02/01/2025 To 02/28/2025

CC - Clarendon College District

Year	Beginning Balance	Refunds	Adjustment	Base Tax	Discounts	Penalty/ Interest	Attorney Fee	Other Payment	Total Paid	Total Due
2003	\$823.68	\$0.00	\$0.00	\$0.83	\$0.00	\$2.16	\$0.60	\$0.00	\$3.59	\$822.85
2015	\$4,591.89	\$0.00	\$0.00	\$0.66	\$0.00	\$0.79	\$0.29	\$0.00	\$1.74	\$4,591.23
2016	\$5,235.60	\$0.00	\$0.00	\$3.60	\$0.00	\$3.92	\$1.51	\$0.00	\$9.03	\$5,232.00
2017	\$7,313.34	\$0.00	\$0.00	\$41.62	\$0.00	\$40.22	\$16.36	\$0.00	\$98.20	\$7,271.72
2018	\$7,207.67	\$0.00	\$0.00	\$9.80	\$0.00	\$8.33	\$3.62	\$0.00	\$21.75	\$7,197.87
2019	\$8,463.11	\$0.00	\$0.00	\$16.33	\$0.00	\$11.92	\$5.64	\$0.00	\$33.89	\$8,446.78
2020	\$8,552.87	\$0.00	\$0.00	\$33.22	\$0.00	\$20.04	\$10.67	\$0.00	\$63.93	\$8,519.65
2021	\$9,916.65	\$0.00	\$0.00	\$60.83	\$0.00	\$29.25	\$18.02	\$0.00	\$108.10	\$9,855.82
2022	\$16,159.09	\$0.00	\$0.00	\$310.03	\$0.00	\$113.25	\$84.69	\$0.00	\$507.97	\$15,849.06
2023	\$28,099.82	\$0.00	\$0.00	\$3,127.81	\$0.00	\$757.07	\$777.05	\$0.00	\$4,661.93	\$24,972.01
2024	\$101,216.32	\$0.00	\$0.00	\$35,300.70	\$0.00	\$422.93	\$2.53	\$0.00	\$35,726.16	\$65,915.62
TOTALS	\$197,580.04	\$0.00	\$0.00	\$38,905.43	\$0.00	\$1,409.88	\$920.98	\$0.00	\$41,236.29	\$158,674.61
CURRENTS	\$101,216.32	\$0.00	\$0.00	\$35,300.70	\$0.00	\$422.93	\$2.53	\$0.00	\$35,726.16	\$65,915.62
DELINQUENTS	\$96,363.72	\$0.00	\$0.00	\$3,604.73	\$0.00	\$986.95	\$918.45	\$0.00	\$5,510.13	\$92,758.99

40-Clarendon College Jurisdiction Totals Summary

1710 Avenue F NW

Report for Month/Tax year February/2025

<u>COLLECTIONS:</u>	<u>FOR MONTH</u>	<u>YEAR TO DATE</u>
CURRENT TAX	\$8,648.17	\$303,837.20
DELINQUENT TAX	\$420.06	\$3,449.23
PENALTY & INTEREST AND ATTORNEY FEES	\$551.76	\$2,189.79
OTHER PAYMENT	\$0.00	\$0.00
TOTAL	\$9,619.99	\$309,476.22
AMOUNT DUE DELINQUENT ATTORNEY	\$136.87	

SIGNED

Tax Assessor

CURRENT		DELINQUENT		OTHER	
LEVY	141,357.47	LEVY	635.37	ATTY FEES	186.07
DISCOUNT		PENALTY	80.53	COURT COST	.00
PENALTY	3,126.11	INTEREST	173.12	ABST FEES	.00
INTEREST	520.81			OTHER FEES	.00
				TOTAL REND PEN	96.41
				(AGENCY PART)	91.58
				(CAD PART)	4.83
TOTAL	145,004.39	TOTAL	889.02	TOTAL	282.48
M&O LEVY	141,357.47	M&O LEVY	635.37		
M&O DISCOUNT		M&O PENALTY	80.53		
M&O PENALTY	3,126.11	M&O INTEREST	173.12		
M&O INTEREST	520.81	M&O TOTAL	889.02		
M&O TOTAL	145,004.39				
I&S LEVY	.00	I&S LEVY	.00		
I&S DISCOUNT	.00	I&S PENALTY	.00		
I&S PENALTY	.00	I&S INTEREST	.00		
I&S INTEREST	.00	I&S TOTAL	.00		
I&S TOTAL	.00				
TOTAL M&O	145,893.41				
TOTAL I&S	.00				
		REF LEVY/PI (MO)	126.52	RET CHK PI ONLY	.80
		REF LEVY/PI (IS)	.00	RET CHK LEVY/PI	.65
		REFUND PI ONLY	.00	RET CHK ATTY	.63
		REFUND LEVY/PI	126.52	RET CHK ABST	.00
		REFUND ATTY	.00	RET CHK COURTS	.00
		REFUND ABST	.00	RET CHK OTHER	.00
		REFUND COURTS	.00	RCK TOT REN PEN	.00
		REFUND OTHER	.00	(AGENCY PART)	.00
		REF TOT REN PEN	.00	(CAD PART)	.00
		(AGENCY PART)	.00		
		(CAD PART)	.00		
DUE TO AGENCY					
DUE TO ATTY					
DUE TO ABST					
DUE TO COURTS					
DUE TO OTHER					
DUE TO REN PEN					
(AGENCY PART)					
(CAD PART)					

I, Christie Johnson, Tax Assessor of the Gray County Tax Office, do solemnly swear that the Summary of Collection made above is true and correct.


CHRISTIE JOHNSON

YEAR	M&O LEVY	M&O PENALTY	M&O INTEREST	I&S LEVY	I&S PENALTY	I&S INTEREST	TOTAL TAXES	ATTY FEES	GRAND TOTAL
2024	141,357.47	3,126.11	520.81	.00	.00	.00	145,004.39	.00	145,004.39
2023	141,374.31	50.05	53.93	.00	.00	.00	478.29	104.27	582.56
2022	156.04	17.85	38.83	.00	.00	.00	212.72	42.13	254.85
2021	19.92	2.41	7.64	.00	.00	.00	29.97	5.98	35.95
2020	18.95	2.26	9.45	.00	.00	.00	30.66	6.12	36.78
2019	8.15	.98	4.96	.00	.00	.00	14.09	2.82	16.91
2018	5.33	.64	3.89	.00	.00	.00	9.86	1.97	11.83
2017	4.06	.49	3.54	.00	.00	.00	8.09	1.64	9.73
2016	29.96	3.60	29.17	.00	.00	.00	62.73	12.58	75.31
2015	12.75	1.54	14.02	.00	.00	.00	28.31	5.70	34.01
2014	1.31	.16	1.58	.00	.00	.00	3.05	.61	3.66
2013	4.59	.55	6.11	.00	.00	.00	11.25	2.25	13.50
2012	.00	.00	.00	.00	.00	.00	.00	.00	.00
2011	.00	.00	.00	.00	.00	.00	.00	.00	.00
2010	.00	.00	.00	.00	.00	.00	.00	.00	.00
2009	.00	.00	.00	.00	.00	.00	.00	.00	.00
2008	.00	.00	.00	.00	.00	.00	.00	.00	.00
2007	.00	.00	.00	.00	.00	.00	.00	.00	.00
2006	.00	.00	.00	.00	.00	.00	.00	.00	.00
2005	.00	.00	.00	.00	.00	.00	.00	.00	.00
2004	.00	.00	.00	.00	.00	.00	.00	.00	.00
2003	.00	.00	.00	.00	.00	.00	.00	.00	.00
2002	.00	.00	.00	.00	.00	.00	.00	.00	.00
2001	.00	.00	.00	.00	.00	.00	.00	.00	.00
2000	.00	.00	.00	.00	.00	.00	.00	.00	.00
1999	.00	.00	.00	.00	.00	.00	.00	.00	.00
1998	.00	.00	.00	.00	.00	.00	.00	.00	.00
1997	.00	.00	.00	.00	.00	.00	.00	.00	.00
1996	.00	.00	.00	.00	.00	.00	.00	.00	.00
PRIOR	.00	.00	.00	.00	.00	.00	.00	.00	.00
TOTAL	141,992.84	3,206.64	693.93	.00	.00	.00	145,893.41	186.07	146,079.48

YEAR TO DATE RECAPULATION FOR AGENCY: CCPC - COLLEGE PAMPA CENTER

LEVY	ORIGINAL	SUPPLEMENTAL	TOTAL CURRENT	% PAID	DELINQUENT	% PAID	SUMMARY
BEGIN	930,080.37	.00	930,080.37		61,591.34		991,671.71
LATE HS/65	238.01-	.00	238.01-		.00		238.01-
OTHER ADJUSTMENTS	2,020.57-	.00	2,020.57-		179.49-		2,200.06-
SUPPLEMENTS	.00	11,319.92	11,319.92		8.93		11,328.85
ADJUSTED	927,821.79	11,319.92	939,141.71		61,420.78		1,000,562.49
COLLECTED	863,041.10-	245.33-	863,286.43-	91.92	6,436.57-	10.47	869,723.00-
PR YR REF/NSF CHK	.00	.00	.00		111.99-		111.99-
UNCOLLECTED	64,780.59-	11,074.59-	75,855.28-		54,872.22-		130,727.50-
LATE RENDITION BEGIN	1,801.70	.00	1,801.70		722.63		2,524.33
LATE REND ADJUSTED	1,780.01	.00	1,780.01		722.63		2,502.64
COLLECTED	863,041.10	245.33	863,286.43	91.92	6,436.57	10.47	869,723.00
LEVY	.00	.00	.00		.00		.00
DISCOUNTS	3,429.25	1.75	3,431.00		785.33		4,216.33
PENALTY	520.52	.29	520.81		1,193.29		1,714.10
INTEREST	866,990.87	247.37	867,238.24		8,415.19		875,653.43
NET	.00	.00	.00		.00		.00
COURT COST	.00	.00	.00		.00		.00
ABST FEES	.00	.00	.00		1,703.12		1,703.12
ATTY FEES	.00	.00	.00		.00		.00
OTHER FEES	.00	.00	.00		19.61		1,650.56
REND PENLTY	1,630.95	.00	1,630.95		18.64		1,568.08
(AGENCY %)	1,549.44	.00	1,549.44		.97		82.48
(CAD %)	81.51	.00	81.51		10,137.92		879,007.11
TOTAL	868,621.82	247.37	868,869.19				
DELINQUENT BREAKDOWN	BEGIN	ADJUSTMENTS	SUPPLEMENTS	ADJUSTED	COLLECTED	PRIOR YR REF	UNCOLLECTED % PAID
2023 -	20,655.46	23.43-	1.21	20,633.24	4,476.47-	111.99-	16,044.78- 21.69
2022 -	10,799.26	24.10-	.98	10,776.14	1,081.60-	.00	9,694.54- 10.03
2021 -	6,145.07	23.01-	.27	6,122.33	372.55-	.00	5,749.78- 6.08
2020 -	5,150.23	22.93-	.66	5,127.96	135.85-	.00	4,992.11- 2.64
2019 -	3,869.12	23.29-	1.03	3,846.86	197.57-	.00	3,649.29- 5.13
2018 -	2,348.41	23.11-	1.00	2,326.30	55.20-	.00	2,271.10- 2.37
2017 -	1,835.97	23.06-	.93	1,813.84	38.61-	.00	1,775.23- 2.12
2016 -	1,597.86	8.09-	.95	1,590.72	40.66-	.00	1,550.06- 2.55
2015 -	2,719.04	7.84-	1.90	2,713.10	19.62-	.00	2,693.48- 0.72
2014 -	2,694.82	.63-	.00	2,694.19	10.12-	.00	2,684.07- 0.37
2013 -	1,690.93	.00	.00	1,690.93	7.89-	.00	1,683.04- 0.46
2012 -	1,139.18	.00	.00	1,139.18	.43-	.00	1,138.75- 0.03
2011 -	418.74	.00	.00	418.74	.00	.00	418.74- 0.00
2010 -	278.49	.00	.00	278.49	.00	.00	278.49- 0.00
2009 -	199.62	.00	.00	199.62	.00	.00	199.62- 0.00
2008 -	49.14	.00	.00	49.14	.00	.00	49.14- 0.00
2007 -	.00	.00	.00	.00	.00	.00	.00 0.00
2006 -	.00	.00	.00	.00	.00	.00	.00 0.00
2005 -	.00	.00	.00	.00	.00	.00	.00 0.00
2004 -	.00	.00	.00	.00	.00	.00	.00 0.00
2003 -	.00	.00	.00	.00	.00	.00	.00 0.00
2002 -	.00	.00	.00	.00	.00	.00	.00 0.00
2001 -	.00	.00	.00	.00	.00	.00	.00 0.00
2000 -	.00	.00	.00	.00	.00	.00	.00 0.00
1999 -	.00	.00	.00	.00	.00	.00	.00 0.00
1998 -	.00	.00	.00	.00	.00	.00	.00 0.00
1997 -	.00	.00	.00	.00	.00	.00	.00 0.00
1996 -	.00	.00	.00	.00	.00	.00	.00 0.00
1995 -	.00	.00	.00	.00	.00	.00	.00 0.00
1994 -	.00	.00	.00	.00	.00	.00	.00 0.00
PRIOR YEARS	-	.00	.00	.00	.00	.00	.00 0.00

Agenda Attachments
For Action Items

Clarendon College
Summary of Investments
2nd Quarter Month Ended 2/28/2025

Investment or Deposit Type	Book Value	Market Value
Publicly Traded Equity and Similar Investments		
Common Stock (U.S. and foreign stocks held in separately managed accounts or internally managed by institution investment staff; exclude mutual or commingled funds)		
Equity/Stock Mutual Funds		
Balanced Mutual Funds (where target allocation is > 50% equities)		
"Commonfund" Equity Commingled Funds		
Other Equity Commingled Funds (if primarily invested in publicly traded equities)		
Preferred Stock		
Other - list by type		
Total Publicly Traded Equity and Similar Investments	0.00	0.00
"Other" Investments - Other than Publicly Traded Equity and Debt Investments		
Real Estate (include direct ownership & investments in real estate limited partnerships, private REITs, or similar vehicles; include a portfolio of publicly traded REITs if managed as a separate asset allocation category rather than comprising part of a broadly diversified stock portfolio)	1,560,000.00	1,500,000.00
Other Real Asset Investments (e.g. investments in infrastructure funds)		
Private Equity		
Hedge Funds		
"Commonfund" Alternative Asset Commingled Funds (Real Estate, Private Equity, Hedge Funds, Commodities, etc.)		
Annuities		
Commodities		
Collectibles		
Other - list by type		
Total "Other" Investments - Other than Publicly Traded Equity & Debt Investments	1,560,000.00	1,500,000.00
Publicly Traded Debt & Similar Investments > 1 year maturity		
U.S. Government Securities ("Treasures")		
U.S. Government Agency Securities ("Agencies")		
Mortgage Pass-Throughs - "Agency"		
Mortgage Pass-Throughs - "Private Label"		
Asset-Backed Securities (ABS) (other than mortgage-backed securities)		
Sovereign Debt (non-U.S.)		
Municipal Obligations	0.00	0.00
Collateralized Mortgage Obligations (CMOs) - list below by category		
Interest Only Strips (IOs)		
Principal Only Strips (POs)		
Inverse Floaters		
Stated Final Maturity longer than 10 years		
Other CMOs - "Agency"		
Other CMOs - "Private Label"		
Corporate Obligations (U.S. or foreign companies) - list below by rating		
Highly Rated (AAA/AA or equivalent)		
Other Investment Grade (A/BBB or equivalent)		
High Yield Bonds (<BBB or equivalent)		
Not Rated (NR)		
Fixed Income/Bond Mutual Funds (longer term; registered with the SEC)		
Balanced Mutual Funds (where target allocation is > 50% bonds or other debt securities)		
"Commonfund" Fixed Income/Bond Commingled Funds		
Other Fixed Income/Bond Commingled Funds (primarily invested in publicly traded debt securities; not registered with the SEC)		
GICs (Guaranteed Investment Contracts)		
Other - list by type		
Total Publicly Traded Debt & Similar Investments > 1 year	0.00	0.00
Short-Term Investments & Deposits		
U.S. Government Securities ("Treasures")		
U.S. Government Agency Securities ("Agencies")		
Bankers' Acceptances		
Highly Rated (AAA/AA or equivalent)		
Asset-Backed Securities (ABS) (other than mortgage-backed securities)		
Other Commercial Paper - lower rated		
Repurchase Agreements (Repos)		

Clarendon College
Summary of Investments
2nd Quarter Month Ended 2/28/2025

Investment or Deposit Type	Book Value	Market Value
Money Market Mutual Funds (registered with the SEC)	6,511,286.79	6,511,286.79
Short-Term Mutual Funds Other than Money Market Mutual Funds (registered with the SEC)		
Public Funds Investment Pool Created to Function as a Money Market Mutual Fund (not registered w/ SEC but "2a7-like")		
TexPool (and TexPool Prime)		
Other Public Funds Investment Pools Functioning as Money Market Mutual Funds	1,765,487.52	1,765,487.52
Other Investment Pools - Short-Term (not created to function as a money market mutual fund)		
Certificates of Deposit (CD) - Nonnegotiable		
Certificates of Deposit (CD) - Negotiable		
Bank Deposits	5,138,153.80	5,138,153.80
Separate Managed Account	2,203.89	2,203.89
Cash Held at State Treasury		
Securities Lending Collateral Reinvestments (direct investments or share of pooled collateral)		
Other - list by type		
Total Short-Term Investments & Deposits	13,417,132.00	13,417,132.00
TOTAL INVESTMENTS and DEPOSITS	14,977,132.00	14,917,132.00
	BOOK VALUE	MARKET VALUE
BEGINNING INVESTMENT ASSET	12,604,762.40	12,544,766.82
Receipts/Contributions	1,000,000.00	1,000,000.00
Investment Income	103,606.42	103,606.42
Distributions- yr. end adj.		
Distributions- Transfer on Investments		
Net Realized Gains (Losses)		
Less previous months Demand Deposit/Balance	(3,869,402.87)	(3,869,402.87)
Changes in Net Unrealized:		
Appreciation: in market value		
(Depreciation)	(1,361.69)	(1,366.11)
Bank Deposits/ Demand Deposits	5,138,153.80	5,138,153.80
Other: Petty Cash on hand	1,373.94	1,373.94
ENDING INVESTMENT ASSETS	14,977,132.00	14,917,132.00

COMPLIANCE STATEMENT
TOTAL INVESTMENTS and DEPOSITS

In accordance with the Clarendon College Investment Policy, the investment officers present this report to the Board of Regents, and state that this report is in compliance with the investment policies and strategies as set forth in the investment policy and the Public Fund Investment Act.

Michael Metcalf
Comptroller

Texas Buckhaults
President

Jim Shelton
Board Member

"INVESTMENT DISCLOSURES"

* Clarendon College employs Edward Jones as the investment advisor.

*Clarendon College does not use soft dollar, directed brokerage or directed commission, commission recapture or any similar arrangements.

*Clarendon College is associated with two foundations:

Mr. Pat Britton, P.O. Box Drawer A, Clarendon, TX 79226 is Chairman of the Clarendon College Foundation and the fair market value of investments as of 8/31/2024 is \$577,658.45..

Mr. Lee Porter, P O Box 632, Pampa, Texas 79066 is the Chairman of the Pampa Center Foundation and the market value of investments as of 1/9/2025 was \$1,422,992.00.

Strictland Estate - Lease information

Type of Land	Lease / Acre	Acres	Total
Farm	\$ 90.00	357.3	\$ 32,158.80
Grass	\$ 40.00	43	\$ 1,720.00
			\$ 33,878.80

OTHER FEES AND DEPOSITS

AGRICULTURE

All Courses (Annual Fee).....	\$30
AGRI 2371, AGRI 2372.....	\$75
AGRI 2121, 2321 (Transportation).....	\$100
All other Agriculture courses except (AGRI 1131, 1325, 1329, 2317)	\$30

ART (Each Course)	\$24
Art Supply Fee (Except ARTS 1303 and 1304) ..	\$64
DELETE	

COMPUTER SCIENCE (Each Course)	\$30
--------------------------------------	------

COSMETOLOGY

Student Permit Fee (First Semester Only).....	\$25
Cosmetology Fee (Per Lab Course).....	Increase
\$15.....	\$75
Cosmo Kit Fee (CSME 1401).....	\$1,500
Increase by \$250	
Lash Kit.....	\$250

DEVELOPMENTAL STUDIES

ENGL, ESOL, MATH, & IRAW, NCBO	\$30
IRAW/NCBO/Dev MATH Course Dev	
Software.....	DELETE
	\$55

DRAMA (Each Course)	\$24
---------------------------	------

FOREIGN LANGUAGES (Spanish & ASL).....	\$24
Spanish (Access Code) INCREASE \$5.....	\$100

INDUSTRIAL MAINTENANCE (Per Course).....	\$75
\$25 Increase	

MATHEMATICS

All Courses (Annual Math XL Fee) ...	INCREASE \$10. \$70
MATH 2342, 2413, 2414, and 2415	\$30

PHYSICAL EDUCATION

PE Activity Transportation Fee (Except 1105, 1110, & 1115).....	\$100
Rodeo (Livestock).....	\$100
PHED 1308, 1309, 1321, 1322	\$24
PHED 1105, 1110, & 1115	\$24

RANCH AND FEEDLOT OPERATIONS

RFO Course Fee.....	\$35
RFO Transportation	\$100
Specialized Schools & Seminars (Fall).....	\$650
Specialized Schools & Seminars (Spring).....	\$650
Technology Fee.....	\$450

SCIENCE

Biology (Except 1322), Horticulture, Physics ...	\$30
Chemistry.....	\$35
HITT 1305 (Access Card).....	DELETE \$125

VOCATIONAL NURSING

Course Fee.....	\$30
Insurance Fee (VN& Intro. to Nursing) (1 st Semester)	
	\$35
Seminar Fee (per semester)	\$45
Assessment (per semester)	\$567
VNSG 1304-Nursing Skills Bag.....	\$300
Phlebotomy Certificate.....	\$168
Intro. to Nursing Certificate.....	\$85

ASSOCIATE DEGREE IN NURSING

Course Fee (Each Course)	\$30
Insurance Fee (1 st Semester Only)	\$35
Assessment (Each Semester).....	\$884
RN Clinical Lab Pack (1st Semester Only).....	\$182

WELDING (Each Course).....	\$200
Increase by \$75	

INTERNSHIP	/	COOPERATIVE
EXPERIENCE.....		\$100

LIVESTOCK AND EQUINE CENTER

Horse Stall Rental....	\$70/Month or \$280/Semester
------------------------	------------------------------

TESTING

TSI (Placement Exam)	\$30
Course Challenge Fee	\$465
Technical Program Assessment Fee (Per Course or Test).....	\$60-\$200
Testing Proctor Fee.....	\$30per hour

Academy COURSES***...NAME CHANGE...0 to \$500

VOCATIONAL NURSING

Permit Fee****	\$180
Board of Nursing Testing Fee****	\$250

**The VCT / ITV / Internet distance education course licensing fee is imposed only when the College incurs charges and/or fees for accessing the Virtual College of Texas, an instructional television site, and/or an Internet course on behalf of a student. These charges vary by course and by site. The actual charges and/or fees are then passed through to the student in the form of a course fee.*

*****Subject to change at the discretion of and payable to the Board of Nursing.*



GOVERNOR GREG ABBOTT

November 13, 2024

Dear University Systems Chairman and Chancellor:

Texans face significant rising costs due to inflation. When inflation and other economic pressures burden household budgets, our public universities must take every step possible to ease the financial burden on our students and their families.

Last year I signed a law that prohibits increasing undergraduate tuition and fees for both the 2023-24 and the 2024-25 academic years.

As this tuition freeze expires, let me be clear: I will not support any tuition increase at any public higher education institution in the upcoming biennium. My office has spoken to the Board of Regents at every public university system, and we are in agreement that no institution in Texas should approve tuition increases for the 2025-26 and 2026-27 academic school years.

The State has made historic investments in higher education, including increased funding for universities and financial aid programs. These efforts reflect our commitment to ensuring that higher education remains accessible and affordable for all Texans. When all Texans have access to quality and affordable education, they can earn better wages, meet workforce qualifications, and experience a higher quality of life. I will ensure college affordability remains a top priority for the state as we head into the next legislative session.

Sincerely,

A handwritten signature in black ink that reads "Greg Abbott". The signature is stylized with a large, flowing "G" and "A".

Greg Abbott
Governor

GA:mw

Resolution of Support

for Continued Investment in the Dynamic Community College Funding Model

Whereas, the State of Texas has demonstrated its commitment to student success and workforce development through the implementation of the outcomes-based funding model established by House Bill 8 during the 88th Legislature;

Whereas, this funding model represents a transformative approach to empowering community colleges to deliver measurable results in alignment with state workforce and educational goals;

Whereas, the funding model prioritizes student outcomes, including the attainment of credentials of value, dual credit opportunities, successful transfer to a four-year university, and support for economically disadvantaged students and adult learners;

Whereas, continued investment in this dynamic funding model will ensure Texas community colleges remain equipped to provide affordable, high-quality education that drives economic growth and mobility;

Whereas, Texas community colleges have requested support for formula funding recommendations made by the Texas Higher Education Coordinating Board for the FY 2026-2027 biennium, alongside a supplemental appropriations request for the current biennium to sustain progress and innovation;

Whereas, amendments to the state funding Performance Tier to include students transferring to private or independent institutions in Texas will strengthen student success pathways and acknowledge the key role these institutions play in the state's higher education and workforce development ecosystem;

THEREFORE, BE IT RESOLVED, the Board of *[Trustees/Regents]* of *[College Name]* officially declares its support for:

1. Continued investment in the outcomes-based funding model established by House Bill 8.
2. Full funding for the supplemental appropriations request for the FY 2024-2025 biennium.
3. Formula funding recommendations for the FY 2026-2027 biennium as proposed by the Texas Higher Education Coordinating Board.
4. Amendments to the Performance Tier to include students who transfer to private or independent institutions of higher education in Texas.

BE IT FURTHER RESOLVED, that this Resolution be included in the permanent minutes of this Board.

ADOPTED THIS ____ day of _____, 2025, by the Board of *[Trustees/Regents]* of *[College Name]*.

[Name], Chair

Board of *[Trustees/Regents]*

[Name], Secretary

Board of *[Trustees/Regents]*

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Acceptable Use Policy:

PURPOSE:

The computing resources at Clarendon College support the educational, instructional, research, and administrative activities of the College, and using these resources is a privilege extended to members of the Clarendon College community. Users of these services and facilities have access to valuable College resources, sensitive data, and internal and external networks. Consequently, it is essential to behave responsibly, ethically, and legally.

In general, acceptable use means respecting other computer users' rights, the physical facilities' integrity, and all pertinent license and contractual agreements. If an individual is found to violate the Acceptable Use Policy, the College will take disciplinary action, up to and including suspension or termination of employment. Individuals are also subject to federal, state, and local laws governing interactions on Clarendon College information technology resources.

This document establishes specific requirements for using all computing and network resources at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202) and Texas Higher Education Coordinating Board)

SCOPE:

The Clarendon College Acceptable Use policy applies equally to all individuals utilizing Clarendon College information technology resources (e.g., employees, faculty, students, retirees, agents, consultants, contractors, volunteers, vendors, temps, etc.).

Information technology resources include all College-owned, licensed, or managed hardware and software and use of the College network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

RIGHTS AND RESPONSIBILITIES:

As college community members, users are provided with scholarly and/or work-related tools, including access to the library, particular computer systems, servers, software, databases, the campus telephone and voice mail systems, and the Internet. There is a reasonable expectation of unobstructed use of these tools, certain degrees of privacy (which may vary depending on whether the user is a College employee or a registered student), and protection from abuse and intrusion by others sharing these resources.

In turn, users are responsible for knowing the regulations and policies of the College that apply to the appropriate use of the College's technologies and resources. Users are responsible for exercising good judgment when using the college's technological and information resources. Just because an action is technically possible does not mean it is appropriate to perform it.

Users are representatives of the Clarendon College community and are expected to respect the College's good name in electronic dealings with those outside the College.

PRIVACY:

All users of College networks and systems should remember that all usage of information technology resources can be recorded and is the property of Clarendon College. Such information is subject to the Texas Public Information Act and the laws applicable to college records retention. Employees have no right to privacy about the use of college-owned resources. Clarendon College management has the ability and right to view employees' usage patterns and act to ensure that College resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on Clarendon College information technology resources owned, leased, administered, or otherwise under the custody and control of Clarendon College are not private. They may be accessed by appropriate personnel by the provisions and safeguards provided in the Texas Administrative Code 1 TAC§202 (Information Security Standards).

ACCEPTABLE USE:

The Clarendon College network supports research, education, and administrative activities by providing access to computing resources and collaborative work opportunities. Primary use of the Clarendon College network must be consistent with this purpose.

Access to the Clarendon College network from any device must adhere to all the same policies that apply to use from within Clarendon College facilities.

1. Users may use only Clarendon College information technology resources for which they are authorized.
2. Users are individually responsible for appropriately using all resources, including the computer, the network address or port, software, and hardware. They are accountable to the College for all use of such resources.
3. Authorized users of Clarendon College resources may not enable unauthorized users to access the network. The College is bound by its contractual and license agreements respecting specific third-party resources; users must comply with all such agreements when using Clarendon College information technology resources.
4. Users should secure resources against unauthorized use or access, including Clarendon College accounts, passwords, Personal Identification Numbers (PINs), Security Tokens (i.e., smartcards), or similar information or devices used for identification and authorization purposes.
5. Users must report shareware or freeware before installing it on Clarendon College-owned equipment unless it is on the approved software list. A request to install software must be reported to the Clarendon College-IT via email before installing any software.

6. Users must not attempt to access Clarendon College information technology resources without appropriate authorization by the system owner or administrator.

RESTRICTIONS:

All individuals are accountable for their actions relating to Clarendon College's information technology resources. Direct violations include the following:

1. Interfering or altering the integrity of Clarendon College information technology resources by:
 - a. Impersonating other individuals in communication;
 - b. Attempting to capture or crack passwords or encryption;
 - c. unauthorized access, destruction, or alteration of data or programs belonging to other users;
 - d. Excessive use for personal purposes, meaning use that exceeds incidental use as determined by supervisor; or,
 - e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.
2. Allowing family members or unauthorized persons to access Clarendon College's information technology resources.
3. Using the Clarendon College information technology resources for private financial gain or personal benefit. Users cannot run private businesses on Clarendon College's information technology resources. Commercial activity is permitted but only for business done on behalf of Clarendon College or its organizations.
4. Activities that would jeopardize the College's tax-exempt status.
5. Using Clarendon College information technology resources for political gain.
6. Using Clarendon College information technology resources to threaten or harass others violating College policies.
7. Intentionally accessing, creating, storing, or transmitting material that Clarendon College may deem to be offensive, indecent, or obscene (other than in the course of academic research or authorized administrative duties where this aspect of the study or work has the explicit approval of the Clarendon College official processes for dealing with academic ethical issues).
8. Not reporting any weaknesses in Clarendon College information technology resources security or any incidents of possible misuse or violation of this agreement by contacting the Information Security Officer.
9. Attempting to access any data or programs on Clarendon College information technology resources for which authorization has not been given.
10. Making unauthorized copies of copyrighted or licensed material.
11. Intentionally using or attempting to introduce worms, viruses, Trojan horses, or other malicious code onto a Clarendon College information resource.

12. Degrading the performance of Clarendon College information technology services; depriving an authorized Clarendon College user access to a Clarendon College information technology resource; obtaining extra information technology resources beyond those allocated; or circumventing Clarendon College security measures.
13. Downloading, installing, or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Clarendon College users must not run password-cracking programs, packet sniffers, port scanners, or any other non-approved programs on Clarendon College information technology services.
14. Engaging in acts against the aims and purposes of Clarendon College as specified in its governing documents or rules, regulations, and procedures adopted by Clarendon College and the Texas State College System.
15. Allowing another person, either through one's computer account or other means, to accomplish any of the above.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Computer Virus: A type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its source code) or infecting other computer programs by modifying them.

Copyright Laws: A form of protection provided by the laws of the United States to authors of "original works of authorship." This includes literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations.

Freeware: Software that is available for use at no monetary cost.

Information Security Officer (ISO): Officer designated to administer the College Information Security Program. Usually, this may be the Vice President of Information Technology.

Malicious Code: A term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

Shareware: A type of proprietary software initially provided free of charge to users, who are allowed and encouraged to make and share copies of the program.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.1. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
IT Administrator/Special Access:

PURPOSE:

This policy aims to provide measures to mitigate information security risks associated with IT Administrators/Special Access.

IT Administrators/Special Access is defined as users with elevated account privileges. Therefore, these privileges must be restricted and granted only to those with an academic or business justification. Administrator accounts and other special-access accounts may have extended and overarching privileges. Thus, the granting, controlling, and monitoring of these accounts is extremely important to the overall Clarendon College information security program. The extent of access privileges granted or used should not exceed that which is necessary. Those employees and/or consultants processing this access will be limited and reviewed annually or as needed.

SCOPE:

The Clarendon College IT Administrator/Special Access Policy applies equally to all individuals who have or may require special access privilege to any Clarendon College information technology resources.

POLICY STATEMENT:

Appropriate security levels and requirements must be determined for all special access accounts that utilize Clarendon College's information technology resources. To safeguard information technology resources, the following controls are required:

1. All Administrative/Special Access account users must have account-management instructions, documentation, and authorization.
2. All users must sign the Clarendon College Non-Disclosure Agreement (see [Clarendon College NDA Policy](#)) and be current on their annual Cybersecurity Awareness Training (see [Clarendon College Technology Security Training Policy](#)).
3. Each individual using special access accounts must use the account privilege most appropriate with work performed (i.e., user account vs. administrator account).
4. Each account used for special access must comply with the "Passwords" guidelines stipulated in the [Clarendon College User Accounts Password Policy](#).
5. The password for a shared special access account must change when an individual with the password leaves the department or Clarendon College or upon a change in the vendor personnel assigned to the Clarendon College contract. The account must also be re-evaluated to determine whether it should remain a shared account. (Shared accounts must be kept to an absolute minimum.)
6. In the case where a system has only one administrator, a password escrow procedure must be in place so that someone other than the administrator can access the administrator account in an emergency.

7. When special access accounts are needed for audit, software development, software installation, or other defined needs, special access must be:
 - a. Authorized by the system owner, Information Resource Manager, or Information Security Officer. (For example, Clarendon College-IT is the system owner of all Clarendon College desktops, laptops, and tablets.)
 - b. Created with a specific expiration date or annual review date.
 - c. Removed when work is complete.
8. All privileged commands issued in association with special access must be traceable to specific individuals via the use of comprehensive logs.

DEFINITIONS:

Information Resources Manager (IRM): Officer responsible for the State of Texas managing Clarendon College's information technology resources.

Information Security Officer (ISO): Officer designated to administer the College Information Security Program.

IT Administrators/Special Access: users with elevated account privileges must be restricted and granted only to those with an academic or business justification.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks to minimize the potential impact of a threat.

Non-Disclosure Agreement (NDA): Formal acknowledgment that all employees must sign, acknowledging they have read and understand Clarendon College's computer security policies and procedures requirements. This agreement becomes a permanent record and will be renewed annually.

System/Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
System Information Technology Services (CLARENDON COLLEGE-IT)
Application Security Policy:

PURPOSE:

The Application Security Policy aims to avoid inadvertent release of confidential or sensitive information, minimize risks to users and the College, and ensure the availability of critical applications.

Clarendon College focuses on security applications that hold or utilize data sets containing student information/records, personally identifiable information such as social security numbers or credit card numbers, and other categories of data protected by federal or state laws or regulations. Ultimately, to ensure application availability and reliability, all applications must be secured regardless of the type of information they utilize.

SCOPE:

The Application Security Policy applies to applications developed by College staff and those acquired from outside providers. All applications are subject to this policy regardless of whether the application is hosted on College equipment or elsewhere.

POLICY STATEMENT:

To keep risk to an acceptable level, Clarendon College shall ensure that the proper security controls will be implemented for each application. Data owners, custodians, system administrators, and application developers are expected to use their professional judgment in managing risks to the information, systems, and applications they use and support. All security controls should be proportional to the confidentiality, integrity, and availability requirements of the data processed by the system.

1. Clarendon College, individual department heads, and contractors shall implement application security standards to have adequate control over systems they directly manage.
 - a. If Clarendon College IT manages an environment or application, it shall be responsible for implementing the application security controls.
 - b. If a department manages an environment or application, that department shall be responsible for implementing the application security controls. The department head will review the policies and all application security controls to ensure they are followed.
 - c. If an outsourced contractor manages a Clarendon College environment or application for an individual department, the department must ensure that the contractor implements the application security controls.

- d. College faculty and staff who engage any third-party hosting services (such as cloud services, SaaS, or managed hosting) for educational, research, or approved purposes must:
 - i. Obtain prior approval from the Vice President of Information Technology or designee.
 - ii. Do not entrust that provider with sensitive or confidential business data as defined in the Data Classification Policy.
 - iii. Availability and support agreements (e.g., 24X7, 8-5, Weekdays only) must be at a level commensurate with the application's expected availability and must be communicated to Clarendon College-IT.
- 2. Applications installed or being changed should follow the standardized application lifecycle established by the Clarendon College-IT Project Lifecycle Policy.
- 3. Each user (whether a developer, administrator, or user) should have unique credentials for accessing a computer application.
- 4. Authenticated users should have access to a computer application and only be allowed to access the information they require (principle of least privilege).
- 5. The application's data owner should approve establishing and changing access for a user or group.
- 6. Developers should follow best practices for creating secure applications, intending to minimize the impact of attacks.
- 7. Developers should not develop or test an application against production data sources.
- 8. Logs for the server, application, and web services should be collected and maintained in a viewable format for a period specified by applicable state regulations.
- 9. Maintain a complete inventory of all applications, including authentication and authorization systems, the data classification, and the criticality level for each application.
- 10. Maintain a written inventory of the data stored within each application.
- 11. Document clear rules and processes for reviewing, removing, and granting authorizations.
- 12. Remove critical authorizations for access to applications for individuals who have left the College, transferred to another department, or assumed new job duties.

13. User access to all applications shall be reviewed annually.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Artificial Intelligence Usage Policy:

PURPOSE:

This policy outlines the acceptable use of Artificial Intelligence (AI) technologies by faculty and students within the college environment. The primary aim is to ensure responsible, ethical, and productive utilization of AI tools while promoting innovation, learning, and academic excellence.

SCOPE:

This policy applies to all faculty, staff, and students who access, use, or interact with AI technologies provided or facilitated by the college, whether on-campus or remotely.

POLICY STATEMENTS:

1. **Alignment with Texas Higher Education Standards:** Must ensure use and compliance with Texas privacy laws, such as the Texas Cybersecurity Act.
2. **Ethical Use:** All faculty and students must utilize AI technologies consistent with ethical standards, respecting human dignity, privacy, diversity, and individual rights.
3. **Accessibility & Accommodations:** Address AI accessibility for students with disabilities in compliance with the Americans with Disabilities Act (ADA). Ensure AI tools used for education are inclusive and support diverse learning needs. AI-driven tools used in coursework, assessments, and administrative functions must comply with Section 508 of the Rehabilitation Act and Web Content Accessibility Guidelines (WCAG) to ensure equal access for students with disabilities. Faculty and staff should verify that AI-generated materials (such as transcripts, summaries, or visual content) are accessible to individuals with vision, hearing, or motor impairments.
4. **Academic Integrity:** The use of AI tools for academic purposes must adhere to the principles of academic integrity. Plagiarism, cheating, or any dishonesty facilitated by AI technologies is strictly prohibited. AI should be used for assistance (e.g., grammar suggestions, summarization) rather than complete content creation. Students are required to disclose AI-assisted work and differentiate between human and AI-generated content.
5. **Legal Compliance:** Users must comply with all relevant laws, regulations, and institutional policies governing the use of AI technologies, including but not limited to data protection, intellectual property rights, and privacy laws.

6. **Training Faculty & Staff on AI Accessibility:** Faculty should be trained to select ADA-compliant AI tools and integrate them into coursework without disadvantaging students with disabilities.
7. **Preventing AI from Creating Accessibility Barriers:** AI-generated content (such as auto-graded assignments or chatbot responses) should not create additional barriers for students with disabilities. If an AI system is used for student assessments or advisement, accommodations should be made for students who require extra support.
8. **AI Use in Administrative Functions:** AI should complement, not replace, human staff in administrative roles. Regular audits of AI systems should be conducted to prevent biases in admissions, grading, or advising.
 - a. **AI Chatbots & Virtual Assistants:** If AI-powered chatbots are used for student inquiries, they should be regularly monitored for accuracy and fairness.
 - b. **AI in Admissions & Financial Aid:** Ensure AI-driven admissions and financial aid decision-making is transparent and does not introduce biases.
 - c. **AI in Student Advising:** AI tools that assist with course selection or career advising should include human oversight to ensure personalized and accurate guidance.
 - d. **Data Privacy & Security:** AI tools handling student data must comply with FERPA (Family Educational Rights and Privacy Act) and Texas data privacy laws.
9. **Responsible Data Handling:** Under applicable privacy regulations, users must handle data responsibly. This includes obtaining necessary permissions for data collection, processing, and sharing and implementing appropriate security measures to protect sensitive information.
10. **Transparency and Accountability:** Faculty and students utilizing AI technologies are responsible for understanding the capabilities and limitations of these tools. They must transparently disclose the use of AI in academic work and be accountable for the outcomes produced. Transparency should be required when AI is making administrative decisions that impact students.
11. **Bias Mitigation:** Users must be vigilant in identifying and mitigating biases inherent in AI algorithms and datasets. They should strive to promote accuracy, fairness, equity, and inclusion in their use of AI technologies.
12. **Intellectual Property Rights:** Users must respect intellectual property rights, including copyrights and patents, when creating, sharing, or using AI-generated content or algorithms.

13. **Professional Development:** The college will provide opportunities for faculty and students to enhance their AI literacy and skills through training, workshops, and other educational resources.
14. **Faculty Guidance and Course Support:** AI's role in the classroom should ensure it enhances learning rather than diminishing academic rigor. AI should be used for assistance (e.g., grammar suggestions, summarization) rather than entire content creation.
- a. **Assignment Design to Deter AI Misuse:** Encourage assignments that require critical thinking, personal reflection, or hands-on experiences that AI cannot easily replicate.
 - b. **AI in Research and Writing:** Syllabi should define when AI-assisted research is appropriate and crosses ethical boundaries (e.g., using AI to generate entire papers).
 - c. **Preventing Over-Reliance on AI:** Faculty should educate students on AI as a tool for enhancement, not a replacement for human learning and effort.
 - d. **Transparency in AI Use:** Syllabi should require students to disclose AI-assisted work and differentiate between human and AI-generated content.
 - e. **Collaborative Learning:** Faculty and students are encouraged to collaborate and share knowledge and resources related to AI technologies in a spirit of academic inquiry and mutual support.
15. **Use in Online and Hybrid Learning:** Faculty should clearly state in their syllabi how AI can or cannot be used in online coursework. AI-generated responses in discussion forums should be disclosed to maintain academic transparency. Any AI-driven tools used in assessments should be vetted for bias and fairness.
- a. **AI in Learning Management Systems (LMS):** Ensure that AI tools used within platforms like Blackboard, Canvas, OpenLMS, or other LMS adhere to academic integrity standards.
 - b. **AI-Generated Assignments:** Course syllabi should define what level of AI assistance (if any) is allowed for assignments, essays, and discussions in online courses.
 - c. **Automated Grading & Feedback:** If AI grading tools are used, ensure they are fair and accurate and provide meaningful feedback.
 - d. **Virtual Proctoring & AI Monitoring:** If AI-powered proctoring tools are used, ensure they do not infringe on student privacy or disproportionately impact certain student groups.
16. **Reporting and Compliance:** Any concerns or incidents related to the misuse or unethical use of AI technologies should be reported to the appropriate authorities for investigation and resolution. The IT department should conduct accessibility audits of AI tools, provide alternative solutions when necessary, and ensure that any AI systems and

services meet the college's Acceptable Use Policy, Security Contracts and Cloud Services Procurement Policy, and the Texas Risk and Authorization Management Program (TX-RAMP) guidelines (<https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp>).

ENFORCEMENT:

Violating this AI use policy may result in disciplinary action, including academic sanctions, loss of privileges, or legal consequences, depending on the severity and nature of the violation.

REVIEW AND MODIFICATION:

This policy will be periodically reviewed and updated as necessary to reflect changes in technology, regulations, and institutional priorities. Amendments to the policy will be communicated to all relevant stakeholders.

ACKNOWLEDGMENT:

By accessing or using AI technologies provided or facilitated by the college, faculty, staff, and students acknowledge their understanding of an agreement to comply with this AI use policy.

DEFINITIONS:

Artificial Intelligence: (AI) is the theory and development of computer systems capable of performing tasks that historically required human intelligence, such as recognizing speech, making decisions, and identifying patterns.

Bias Mitigation: Refers to the proactive process of identifying, addressing, and reducing biases within an organization or society. These biases can manifest in various forms, such as unconscious biases based on race, gender, age, or socioeconomic status.

Texas Risk and Authorization Management Program (TX-RAMP): Provides a standardized approach for security assessment, certification, and continuous monitoring of cloud computing services that process the data of Texas state agencies.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

This policy was approved by the Clarendon College Board of Regents on _____, version 1.0. This policy was reviewed by Will Thompson, Vice President of IT on _____.

Clarendon College
System Information Technology Services CLARENDON COLLEGE-IT)
Authorized Software Policy:

PURPOSE:

Authorized software is any software that is acceptable for use on Clarendon College information technology resources. The Authorized Software Policy aims to provide measures to mitigate information security risks associated with authorized software.

Clarendon College has negotiated special pricing and licensing for software available to all students, faculty, and staff. Other software is readily available in the open marketplace with some licensing agreement under which the user is subject. Some software is considered to pose a security threat to Clarendon College, and its use may be restricted.

Users entrusted with Clarendon College information technology resources are responsible for maintaining licensing information for any software the user installs and, if requested by the College, must provide Clarendon College with licensing information. This includes, but is not limited to, smartphones, iPads, tablets, laptops, etc.

Non-compliance with copyright laws regarding software is subject to civil and criminal penalties imposed by federal and state laws. These penalties apply to the College and/or an individual.

SCOPE:

The Authorized Software Policy applies to all Clarendon College information technology resource users.

POLICY STATEMENT:

All software installed or used on College-owned information technology resources must be appropriately licensed.

Clarendon College-IT shall maintain sufficient documentation to validate that the software is appropriately licensed. Persons installing or authorizing software installation should be familiar with the terms of the agreement.

Users shall accept the responsibility to prevent illegal software usage and abide by College policy on using copyrighted materials, requiring the College community to respect copyright law. These responsibilities include:

1. Do not illegally distribute or share software with anyone.
2. All software must be license-compliant, including personally purchased software.
3. All software licenses must be readily available.
4. Report any suspected or known misuse of software to Clarendon College-IT.

The following general categories of software are prohibited explicitly on all Clarendon College Information Technology Resources unless specifically authorized by the Information Security Officer:

1. Software used to compromise the security or integrity of computer networks and security controls, such as hacking tools, password descramblers, network sniffers, and port scanners.
2. Software that proxies the authority of one user for another to gain access to systems, applications, or data illegally.
3. Software instructs or enables users to bypass normal security controls.
4. Software that instructs or enables the user to participate in any activity considered a threat to local, state, or national security, including the assistance or transfer of information leading to terrorist activity or construction or possession of illegal weapons.
5. Any other software prohibited explicitly by the Information Security Officer.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Business Continuity and Disaster Recovery Policy:

PURPOSE:

Business continuity (BC) goes further than traditional Backup and Disaster Recovery (BDR) strategies. BDR plans are built chiefly around contingencies should something fail. They are more reactive than proactive. A good BC strategy includes a BDR strategy, but it also incorporates a highly redundant system architecture to ensure that systems are resilient and built out to be highly available.

SCOPE:

All Clarendon College centers will adhere to this policy. All critical servers are located at the main campus in Clarendon, the Pampa Center in Pampa, and the Childress Center in Childress. All business-critical server backups are hosted in the Runbiz Austin data center. The Austin facility boasts a Tier IV datacenter rating, which is the highest achievable.

The Run Biz data center is equipped with the following redundancies:

1. Redundant power routes from different providers
2. Redundant Battery Backup (UPS)
3. Redundant HVAC Cooling
4. Three internet paths for secondary and tertiary failover
5. Reinforced physical structure, including concrete bollards and steel-lined wall options for security, and bullet-resistant glass

Furthermore, critical applications are hosted on the following:

1. Redundant Server Hosts – an entire physical server can be lost and operations can continue
2. Redundant Storage – all data is stored in a very resilient storage solution that guarantees no data loss due to disk failure

POLICY STATEMENT:

1. Servers are backed up hourly in the Austin data center to a local set of disks.
2. all backups are copied offsite to the Las Vegas data center each evening. The LV data center is equipped with standby disaster recovery hardware. Should a catastrophic event result in the loss of the Austin data center, all Runbiz servers can be recovered to the backup from the previous night. The servers can then be brought online in the Las Vegas data center. College-wide access can be restored in 24 to 48 hours. See Appendix A and C for diagram explanations of the process.
3. See the Data Backup Policy for data backup details.
4. Communication Response Procedures:
 - a. During a disaster, the Disaster Response Team at Clarendon College will be activated. The Disaster Response Team will be composed of the following Clarendon College employees:
 - 1) College President, team lead,

- 2) Vice President of Academics Affairs, academic records lead,
 - 3) Comptroller, purchasing and insurance lead,
 - 4) Vice President of Student Affairs, student records lead,
 - 5) Vice President of IT, systems management lead,
 - 6) Director of Maintenance, facilities lead,
 - 7) In addition, site assistance members, depending on the location of the disaster.
 - 8) Other staff members as deemed necessary during the disaster.
- b. All Disaster Response team members will be contacted in the above order immediately.
 - c. During a disaster, a communications channel will be opened for Run Biz. The channel is to include the following persons:
 - 1) John McKee, vCIO
 - 2) Bob Talley, Customer Success Manager
 - 3) Kevin Winkle, Solutions Manager
 - 4) Toby Giddens, President
 - 5) 2 Available IT engineers
 - d. The college's Internet and phone service providers will be contacted if communications are affected.
 - 1) Campus or Center ISP service provider
 - i. Main Campus/Childress and Amarillo, AMA Techtel
 - ii. Pampa Center, Vexus
 - iii. Childress Center, Santa Rosa Communications
 - iv. Amarillo Center, AMA Techtel
 - 2) Campus or Center phone service provider
 - i. Main Campus/Amarillo and Pampa, AMA Techtel
 - ii. Childress, Santa Rosa Communications
 - e. Thesis and 3D Technologies will be contacted if CAMS has been affected by the disaster.
 - f. Dynavistics will be contacted if Dynamics GP has been affected by the disaster.
 - g. See Appendix B of this policy for listing all major IT vendors for Clarendon College and their contact numbers.
5. Critical Systems:
 - a. CAMS Enterprise
 - b. Dynamics GP – ERP / Accounting Data
 - c. File Server
 - d. Domain Controllers/DNS
 - e. PBX Phone Server
 - f. Remote Access Servers / Terminal Servers
 - g. Printing

Recovery procedures:

1. Servers will be restored in order of importance as outlined above with the following procedures:
 - a. Identify the latest recoverable restore point on the backup appliance
 - b. Initialize recovery wizard

- c. Select "Volume Restore"
 - d. Select Hyper-V host as the destination
 - e. Keep original Resources levels
 - f. Initialize Recovery
 - g. Once the VM is online, perform a test login to the operating system
 - h. Confirm that the system is online with a route to the internet
 - i. Configure the firewall to allow access back to the internal server
2. PCs, Internet, network, and phone services will be reallocated and restored according to the following areas and or prioritized as listed below;
- a. Administration
 - b. Business Services
 - c. Student Services
 - d. Academic Services
 - e. Instructional Services
 - f. Athletics
 - g. Maintenance/Custodial/Automotive Services

Equipment Replacement:

Old PCs and servers will be operational until new systems can be ordered and deployed for restoration.

Telephone Communications:

Until phone services are restored, the college will rely on mobile phone service.

DEFINITION:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Cloud Storage: A service model in which data is maintained, managed, backed up remotely, and made available to users over the Internet.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

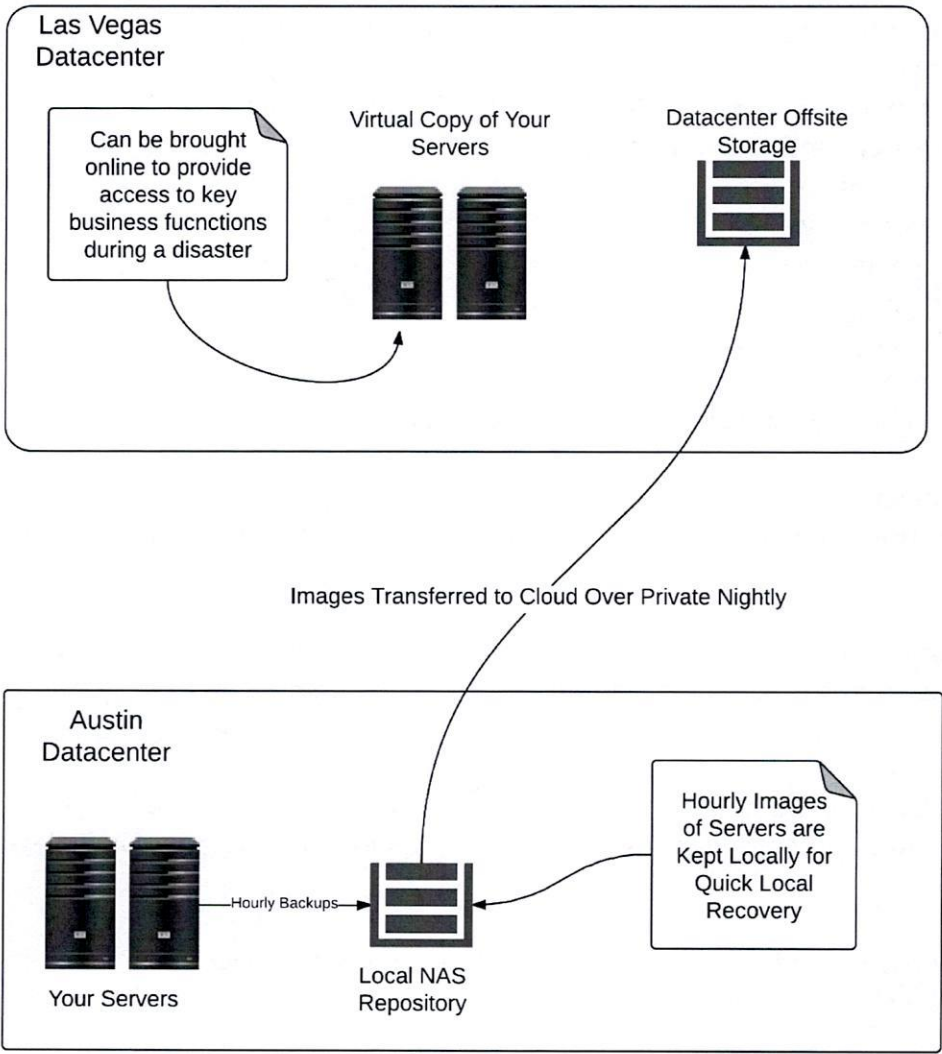
The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

APPENDIX A.

Offsite Backup:

The diagram below depicts the backup methodology from Austin to Las Vegas.



The Clarendon College Board of Regents approved this policy on _____, version 1.2.
This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

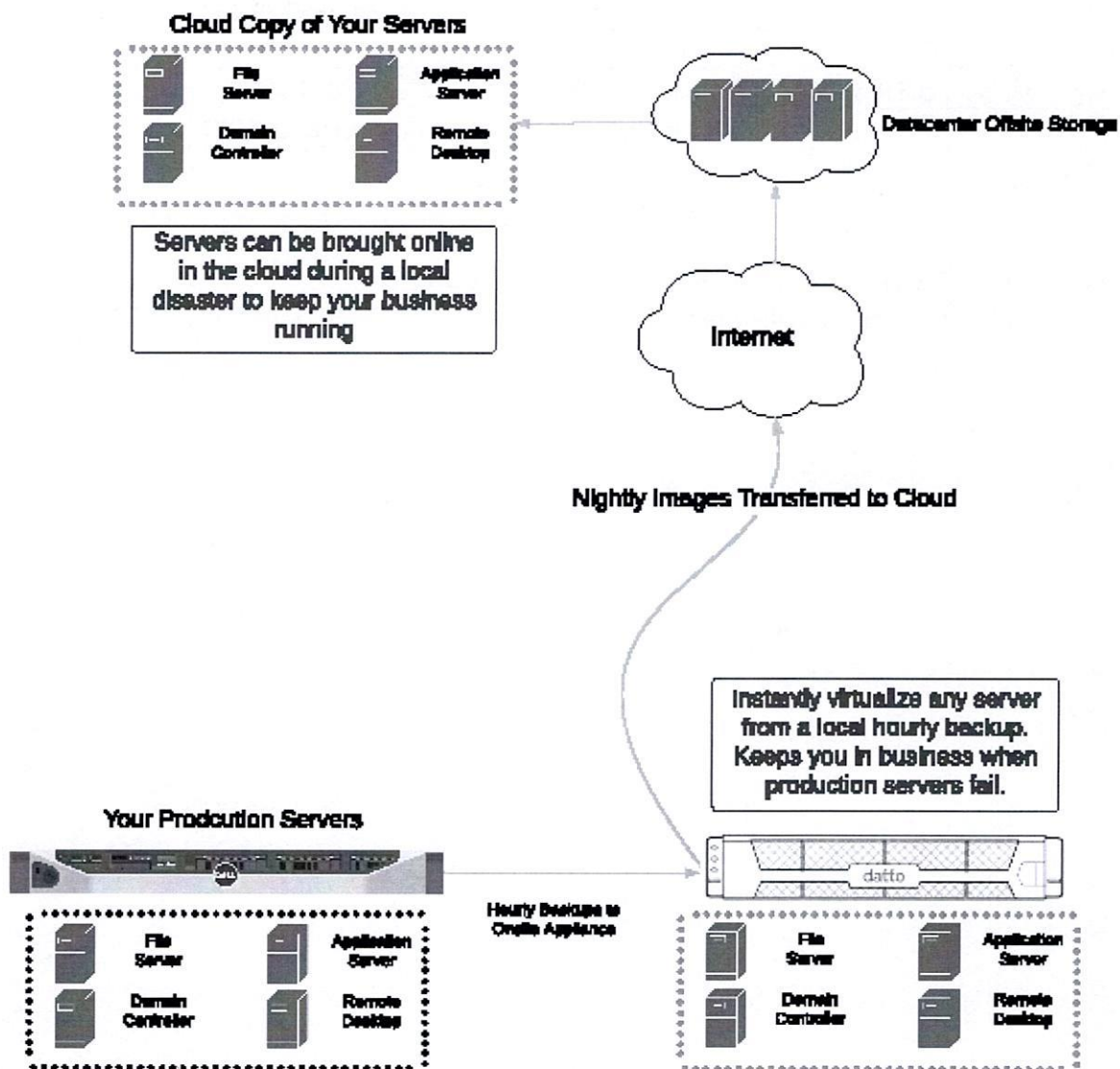
APPENDIX B.

Vendor phone listing.

Agency	Area of Operation	Phone Number
Run Biz	General Tech Support	806-322-2150
AMA Techtel	ISP, (AM, CC, CH)	806-322-2222
AMA Techtel	Phone Provider (AM, CC, PA)	806-322-2222
Vexus	ISP (PA)	877-469-2251
Santa Rosa	ISP/Phone Provider(CH)	888 844-0540
Thesis	CAMS Enterprise	636 779-1522
3D Technologies	CAMS Enterprise	816 505-9845
Herring Bank, Financial Payments	Banking and Online Payments	806 242-3740
Tim Moreland	TV System	806 282-7948
Dynavistics	Dynamics GP	
DRI	Smart Room Systems	

The Clarendon College Board of Regents approved this policy on _____, version 1.2.
This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Business Continuity and Disaster Recovery



The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Personally-Owned Device Usage Policy

PURPOSE:

This policy applies to any hardware and related software not owned or supplied by Clarendon College but could be used to access Clarendon College resources. This applies to all Clarendon College agents who have personally acquired a device but also wish to use this device in the business environment.

SCOPE:

All users employing a personally owned device connected to the Clarendon College network and/or capable of backing up, storing, or accessing any college data must adhere to college-defined policies, standards, and processes.

PRIVACY:

All users of College networks and systems should remember that all usage of information technology resources can be recorded and is the property of Clarendon College. Such information is subject to the Texas Public Information Act and the laws applicable to college records retention. Employees have no right to privacy about the use of college-owned resources. Clarendon College management has the ability and right to view employees' usage patterns and act to ensure that College resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on Clarendon College information technology resources owned, leased, administered, or otherwise under the custody and control of Clarendon College are not private. They may be accessed by appropriate personnel following the provisions and safeguards provided in the Texas Administrative Code 1 TAC§202 (Information Security Standards).

GUIDELINES FOR ACQUISITION AND USE:

Employees and other agents must appropriately secure the device to prevent data from being lost or compromised, reduce the risk of spreading viruses, and mitigate other forms of abuse to the college's computing infrastructure by following security guidelines.

- a. Employ some device access protection such as, but not limited to, strong passcode, facial recognition, card swipe, fingerprint, etc.
- b. Set an idle timeout that will automatically lock the device if misplaced.
- c. Keep the device's software (operating, anti-virus, security, encryption, etc.) up-to-date.
- d. Enroll your device in "Find my phone" or similar services and/or label your device with some identifying information (work or home phone number, name, and or

address) to make the device easy to return if lost or stolen; this may be done via your locked screen.

- e. Report any incident or suspected incidents of unauthorized data access, data or device loss, and/or disclosure of system or participant organization resources related to personally owned devices immediately to your manager. (Managers will immediately report such incidents to the Clarendon College Vice President of Information Technology).

Sensitive and private data must not be stored on these devices or external cloud-based personal accounts like Office365, Dropbox, or Box.net.

When using the personally owned device for college business is no longer required, the employee will provide documentation to their manager acknowledging and confirming that the device does not contain any Clarendon College sensitive data.

Employees and other agents must:

- a. Complete the Cyber Security Training
- b. Sign and return the Clarendon College Non-Disclosure Agreement.

ADDITIONAL CONSIDERATIONS:

Employees using prior approved personally owned devices may not be reimbursed by the college for purchase or monthly service expenses unless authorized by the college president.

The college will not reimburse loss, theft, or damage to personally owned devices. This includes, but is not limited to, when the device is used for college business, on college time, or during business travel.

Personally Owned devices used to access, store, back up, or relocate any college or client-specific data may be subject to the search and review due to litigation involving the college and by the State of Texas Open Records Act.

Clarendon College reserves the right to implement technology to remove college-owned data and monitor access to identify unusual usage patterns or other suspicious activity. This monitoring may be necessary to identify accounts/computers that external parties may have compromised.

Failure to comply with Clarendon College's BYOD Policy may result in suspending all technology use and connectivity privileges, disciplinary action, and/or possible termination of employment.

DEFINITIONS:

Bring Your Own Device (BYOD): Refers to employees taking their device to work, Whether laptop, smartphone, or tablet, to interface with the internal/participant organization's network resources. This also refers to mobile storage devices such as USB and external hard drives.

Confidential Data: Data for which restrictions on the accessibility and dissemination of information are in effect. This includes information whose improper use or disclosure could adversely affect the ability of the institution to accomplish its mission, records about individuals requesting protection under the Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act (HIPPA), PCI standards, as well as, data not releasable under the Texas Open Records Act, the Texas Open Meetings Act, or some other statute.

Public Data: Data elements with no access restrictions are available to the general public. This data can also be designated as unrestricted data.

Prior Approval: A process by which all users must gain approval before working with, utilizing, or implementing a process or procedure.

Sensitive Data: Data for which users must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the participant organization. Examples: Personal Identifiable Information (PII), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA) PCI standards, as well as data not releasable under the Texas Open Records Act, the Texas Open Meetings Act, or some other statute.

Use: Use includes accessing, inputting, processing, storing, backing up, or relocating any Clarendon College or client-specific data, as well as connecting to a network.

Devices: Devices include smartphones, tablets, laptops, desktops, and mobile storage devices such as USB drives, external hard drives, etc.

Agents: Agents include employees, including full- and part-time staff, students, consultants, and other agents.

RELATED POLICIES, REFERENCES AND ATTACHMENTS:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website. Also, please see the following related policies below;

- a. Clarendon College's Acceptable Use Policy
- b. Clarendon College's Authorized Software Policy

The Clarendon College Board of Regents approved this policy on _____, version 1.1. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Information Technology Change Management Policy:

PURPOSE:

Each information technology resource element occasionally requires an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may result in upgrades, maintenance, or fine-tuning. Managing these changes is critical to providing a robust and valuable infrastructure for information technology resources.

The Information Technology Change Management policy aims to manage changes rationally and predictably so Clarendon College constituents can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce the negative impact on the user community and to increase the value of Information Technology Resources.

SCOPE:

The Clarendon College Information Technology Change Management policy applies to all individuals who install, operate, or maintain Clarendon College's information technology resources.

POLICY STATEMENT:

1. Changes to Clarendon College information technology resources such as operating systems, computing hardware, networks, and applications are subject to this policy. They must follow the Clarendon College-IT Change Management Procedures.
2. All changes affecting computing environmental facilities (e.g., air- -conditioning, water, heat, plumbing, electricity, and alarms) must be reported to or coordinated with the Information Resource Manager (IRM).
3. A Change Advisory Board (CAB) appointed by the designated IRM must regularly review change requests and ensure that change reviews and communications are satisfactorily performed.
4. A formal written change request or email must be submitted to the IRM for all scheduled and unscheduled changes.
5. All scheduled change requests must be submitted following change management procedures so that the CAB has time to review the request, determine and review potential failures, and decide whether to allow or delay the request.
6. The CAB will assess the change's urgency and impact on the infrastructure, end-user productivity, and budget.

7. Each scheduled change request must receive formal CAB approval before proceeding.
8. The appointed IRM liaison of the CAB may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change will negatively impact a key business process, or if adequate resources cannot be readily available.
9. The CAB works with the change requestor to develop a specific justification for the change and to identify how the change may impact the infrastructure, business operations, and budget. The CAB uses this information to further research and develop a risk and impact analysis. When completing the change analysis, the CAB must consider the business and the technical impacts and risks.
10. System owners and/or system administrators may appeal a denied CAB change request to the IRM.
11. The IRM will convene the impacted members of the CAB, system owners, system administrators, and other stakeholders, as agreed by the IRM and System Owner(s), to decide whether to implement the requested change.
12. Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.
13. A Change Review must be completed for each change, whether scheduled or unscheduled, or successful.
14. A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
 - a. Date of submission and date of change;
 - b. Owner and custodian contact information;
 - c. Nature of the change; and
 - d. Indication of success or failure, including lessons learned.

DEFINITIONS:

Change Advisory Board: CAB comprises management and technical teams that meet regularly to review change requests.

Change Control: A formal internal control procedure to predictably manage changes so Clarendon College IT and constituents can plan accordingly.

Change Review: A method involving analyzing the problem, recommended solution, and back out procedure. Implementation should be monitored to ensure security requirements are not breached or diluted.

Information Resources Manager (IRM): Officer responsible for the State of Texas managing Clarendon College's information technology resources. Usually, this is the Vice President of Information Technology. If this position is vacant, it will fall to the college president.

Outage: Planned or unplanned unavailability or decrease in quality of service due to expected downtime because of upgrades or maintenance or unexpected incidents.

System/Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix A

Change Advisor Board Members:

1. Vice President of Information Technology
2. Vice President of Academic Affairs
3. Registrar

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Cloud Computing Policy

Cloud computing offers several advantages, including low costs, high performance, and quick delivery of services. However, without adequate controls, this service also exposes employees and the college to many online threats, such as data loss or theft and unauthorized access to college networks.

PURPOSE:

This cloud computing policy ensures that cloud services are NOT used without the Vice President of Information Technology (IT) knowledge and approval. Because of the possible threats, it is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation, or exchange of college-related communications or college-owned data without the Vice President of IT's input. This is necessary to protect the integrity and confidentiality of Clarendon College data and the security of the college's network.

Clarendon College's IT department remains committed to enabling employees to do their jobs as efficiently as possible through technology and providing a platform for student learning and achievement. The following guidelines are intended to establish a process whereby college employees can use cloud services without jeopardizing college data and computing resources.

SCOPE:

This policy applies to all employees in all departments of Clarendon College, with no exceptions.

This policy pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts not used to conduct college business are excluded.

If you are not sure whether a service is cloud-based or not, please get in touch with the IT department.

POLICY:

1. The Vice President of IT must formally authorize using cloud computing services for work purposes. The Vice President of IT will certify that the cloud-computing vendor will adequately address security, privacy, and all other IT management requirements.
2. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Vice President of IT.
3. Such services must comply with the college's existing Acceptable Use Policy/Privacy Policy/BYOD Policy.

4. All cloud-computing services must be pre-approved before usage. Pre-approval can be done via email to the Vice President of IT. The email request should mention why the service is needed, how the service will be used, the web URL, and the administrative login used for the service, following the college's Acceptable Use Policy.
5. Employees must not share login credentials with co-workers. The IT department will keep a confidential document containing account information for business continuity purposes.
6. Such services must comply with all laws and regulations governing handling personally identifiable information, college financial data, or any other data owned or collected by Clarendon College.
7. The Vice President of IT decides what data may or may not be stored in the Cloud.
8. Personal cloud services accounts may not be used to store, manipulate, or exchange college-related communications or college-owned data.

PRE-APPROVED CLOUD COMPUTING SERVICES:

Vendor	URL
Office 365	https://www.office.com/
OpenLMS	https://cctx.mrooms.net/login/index.php
LoudCloud	https://bned.loudcloudsystems.com/learningPlatform/user/login.lc
MathXL	https://www.pearsonmylabandmastering.com/northamerica/mathxl/
Pearson VUE	https://navigator.pearsonvue.com/Navigator/authenticate/login
Yuja	https://clarendoncollege.yuja.com/
Global Learning Systems	https://clarendoncollege.glsondemand.com/login?ReturnUrl=%2f
Zoom	https://www.zoom.us/
Cengage	https://login.cengagebrain.com/cb/
Cengage Dashboard	https://www.cengage.com/dashboard/#/login
APPS	https://www.eselfserve.com/login_ess.php
Device Magic	https://www.devicemagic.com/users/login
Evolve	https://evolve.elsevier.com/cs/
HESI	https://hesiinet.elsevier.com/
ATI	https://www.atitesting.com/
Khan Academy	https://www.khanacademy.org/
Shopify	https://www.shopify.com/
Hawkes Learning	http://www.hawkeslearning.com/
Brainfuse	http://home.brainfuse.com/
Harrington Library	https://hrlc.ent.sirsi.net/client/en_US/ccl/
Yodeck	https://app.yodeck.com
PrestoSports	http://prestosports.com/landing/index

Cloudcard	https://app.onlinephotosubmission.com/#/admin
Openstax	https://openstax.org/
SaplingLearning	https://openstax.org/
Tawk.to	https://dashboard.tawk.to/#/dashboard
GFCGlobal	https://edu.gcfglobal.org/en/
Turnitin	https://www.turnitin.com/
ATLO	https://txclarendon.corrlms.com/
Keeper	https://keepersecurity.com/vault/#

The college's IT department handles account management for the above services. Don't hesitate to contact IT to request an account for the above services.

DEFINITIONS:

Clarendon College IT: the department or any company working on behalf of the Clarendon College IT Department responsible for maintaining and supervising the Clarendon College IT infrastructure.

Cloud Service: any service made available to users on demand via the Internet from a cloud computing provider's server instead of being provided from the college's on-premises servers.

Software-as-a-Service (SaaS): a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS).

Infrastructure-as-a-Service (IaaS): online services that provide high-level APIs used to point to various low-level details of underlying network infrastructure like physical computing resources, location, data partitioning, scaling, security, backup, etc. A hypervisor runs the virtual machines as guests, such as Xen, Oracle VirtualBox, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V, LXD.

Platform-as-a-Service (PaaS): a cloud computing offering in which a service provider delivers a platform to clients, enabling them to develop, run, and manage business applications without the need to build and maintain the infrastructure such software development processes typically require.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on July 15, 2023.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Electronic Communication Policy:

INTRODUCTION:

Clarendon College encourages using electronic communications to share information and knowledge to support the college's mission of education and conduct the college's business. To this end, the college supports and provides interactive electronic communications resources and facilities for telecommunications, mail, publishing, and broadcasting. Recognizing the convergence of technologies based on voice, video, and data networks, this Policy establishes an overall policy framework for electronic communications.

PURPOSE:

Electronic communication transfers text, HTML, images, or data through a computer, cell phone, tablet, handheld electronic device, or other communication device. This includes E-mail, instant messaging, texting, web pages, social media, digital signage, blogs and forums.

Clarendon College's electronic communication services support educational and administrative activities and serve as a means of official communication by and between users and Clarendon College. This policy aims to ensure that these critical services remain available and reliable and are used for purposes appropriate to the College's mission.

This policy is recognized to establish prudent and acceptable practices regarding electronic communication and to educate individuals using it concerning their responsibilities associated with such use.

SCOPE:

This policy applies to all members of the Clarendon College community who are entitled to electronic communications to send, receive, or store electronic messages.

POLICY STATEMENT:

Under the provisions of the Information Resources Management Act (Texas Government Code, Title 10, Subtitle B, chapter 2054), information technology resources are strategic assets of the State of Texas that must be managed as valuable state resources.

Clarendon College provides electronic communication services to faculty, staff, students, and other affiliated classes of individuals, including retirees and official visitors. The use of Clarendon College's electronic communication services must be consistent with Clarendon College's educational goals and comply with local, state, and federal laws and College policies.

Communications via Clarendon College electronic systems are the property of Clarendon College, and management maintains the right to access when necessary. All user activity on Clarendon College information technology resource assets is subject to logging, review, and opening records.

Electronic communication must comply with the Clarendon College Acceptable Use, Digital Encryption, and Email Usage policies.

All members of the Clarendon College community are responsible for actively monitoring their voicemail, email, and Microsoft Teams messages during school work days. Faculty, staff, and students must check their official email addresses frequently and consistently to stay current with College communications. The College recommends checking email at least once a day in recognition that certain communications may be time-critical. (Also referenced in the Clarendon College Email Usage Policy.)

The following activities are prohibited as specified by the Texas Department of Information Resources in response to TAC §202 requirements:

1. Sending electronic communication that is intimidating or harassing.
2. Using electronic communication to transmit or receive material that may be offensive, indecent, or obscene.
3. Using electronic communication for conducting personal business.
4. Using electronic communication for purposes of political lobbying or campaigning.
5. Violating copyright laws by inappropriately distributing protected works.
6. Posing as anyone other than oneself when sending electronic communication, except when authorized to send messages for another when serving in an administrative support role.
7. Sending or forwarding chain letters.
8. Send unsolicited messages to large groups except as required to conduct college business.
9. Sending messages with huge attachments.
10. Sending or forwarding electronic communication likely to contain computer viruses, malware, spyware, or other malicious software.
11. Transmitting electronic messages, material, or emails containing sensitive college or personal data insecurely over an external network. (All sensitive material **must** be securely transmitted or encrypted during transmission; see Digital Encryption Policy.)
12. Electronic communication users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Clarendon College or any unit of Clarendon College unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing Clarendon College. An example of a simple disclaimer is: "The opinions expressed are my own and not necessarily those of my employer."

DEFINITIONS:

Computer Virus: A type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its source code) or infecting other computer programs by modifying them.

Copyright Laws: A form of protection provided by the laws of the United States to authors of "original works of authorship." This includes literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations.

Disclaimer: A statement that something isn't authentic or someone isn't responsible. For example, "the opinions expressed are my own, not necessarily those of my employer."

Encryption: Converting information or data into a code to prevent unauthorized access.

Electronic Communication: Electronic communication transfers text, HTML, images, or data through a computer, cell phone, tablet, HANDHELD ELECTRONIC DEVICE, or other communication device. This includes E-mail, instant messaging, texting, web pages, social media, digital signage, blogs and forums.

Malicious Software: Malicious software, commonly known as malware, harms a computer system.

Malware: Any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Sensitive Data: Information that is protected against unwarranted disclosure. Access to sensitive information should be safeguarded.

Social Media: Computer-mediated technologies that facilitate the creation and sharing of information, ideas, career interests, and other forms of expression via virtual communities and networks.

Spyware: Software that aims to gather information about a person or organization without their knowledge, may send such information to another entity without the consumer's consent, or asserts control over a device without the PC user's knowledge.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2.
This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (Clarendon College-IT)
Data Access Review Policy:

PURPOSE:

The Clarendon College Guidelines for Data Standards, Data Integrity, and Security document designate authority and responsibility for the ownership of College enterprise operational data. Commensurate with these defined roles, the specified Data Owners and Data Custodians are responsible for maintaining information security by establishing controls to confirm compliance with official procedures and policies.

SCOPE:

The Clarendon College Data Access Review policy applies equally to all Data Owners and Data Custodians.

POLICY STATEMENT:

The following distinctions among owner, custodian, and user responsibilities guide the determination of the roles:

Data Owner

The owner or their designated representative(s) are responsible for:

1. classifying information under their authority, with the concurrence of the Clarendon College President or their designated representative(s), following Clarendon College's established information classification categories;
2. approving access to information resources and periodically review access lists based on documented risk management decisions;
3. formally assigning custody of information or an information resource;
4. coordinating data security control requirements with the ISO;
5. conveying data security control requirements to custodians;
6. providing authority to custodians to implement security controls and procedures;
7. justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the Clarendon College information security officer and
8. participating in risk assessments as provided under §202.75 of the Texas Administrative Code.

Data Custodian

Custodians of information resources, including third-party entities providing outsourced information resources services to Clarendon College, shall:

1. implement controls required to protect information and information resources needed for this program based on the classification and risks specified by the information owner(s) or as determined by the policies, procedures, and standards defined by the Clarendon College Information Security Program;
2. provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

3. adhere to monitoring techniques and procedures approved by the ISO for detecting, reporting, and investigating incidents;
4. provide information necessary to provide appropriate information security training to employees and
5. ensure information is recoverable following risk management decisions.

Users

The user of an information resource has the responsibility to:

1. use the resource only for the purpose specified by Clarendon College or the information owner;
2. comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
3. formally acknowledge that they will comply with the security policies and procedures in a method determined by the Clarendon College President or their designated representative.

Data Owners and Data Custodians must:

1. No less than annually, document a complete review of parties accessing data under their area of responsibility.
2. Ensure data access reviews are performed more periodically, as deemed necessary by the Data Owner, relative to the risk of the data accessed.
3. Ensure any staffing changes are reflected as necessary to access authorizations promptly.
4. Promptly review, grant, or deny data access requests as appropriate based on essential College documented needs.
5. Ensure any user data access changes comply with the Change Management Policy.
6. Ensure controls are established as required or deemed necessary by the Data Owner to maintain information security.
7. Maintain documentation of compliance with this policy.

Information Security Officer (ISO)

Clarendon College shall have a designated Information Security Officer (ISO) and shall provide that its Information Security Officer reports to executive-level management, has the authority for information security for the entire college, and possesses the training and experience required to administer the functions described below.

The ISO is responsible for:

1. developing and maintaining a college-wide information security plan as required by §2054.133, Texas Government Code;
2. developing and maintaining information security policies and procedures that address the requirements of this program and the institution's information security risks;
3. working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of this program and the institution's information security risks;

4. providing for training and direction of personnel with significant responsibilities for information security concerning such responsibilities;
5. Provide guidance and assistance to Clarendon College senior officials, information owners, information custodians, and end users concerning their responsibilities under this program;
6. ensuring that annual information security risk assessments are performed and documented by information owners;
7. reviewing the Clarendon College inventory of information systems and related ownership and responsibilities;
8. developing and recommending policies and establishing procedures and practices, in cooperation with the Clarendon College Information Resources Manager, information owners, and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure;
9. coordinating the review of the data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data;
10. verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed upon and obligated before the purchase of information technology hardware, software, and systems development services for any new high-impact computer applications or computer applications that receive, maintain, and/or share confidential data;
11. reporting, at least annually, to the Clarendon College President the status and effectiveness of security controls; and
12. Inform the parties in the event of noncompliance with this chapter and/or with Clarendon College's information security policies.

With the approval of the Clarendon College President, the Information Security Officer may issue exceptions to information security requirements or controls in this Program. Any exceptions shall be justified, documented, and communicated during the risk assessment.

Information Resources Manager (IRM) (TAC 211)

The Clarendon College Information Resources Manager (IRM) is responsible to the State of Texas for managing the college's information resources. The designation of the college's Information Resources Manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of Clarendon College's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Clarendon College Information Resources. According to TAC§211, if the IRM position falls vacant, the role defaults to the college President, who is then responsible for executing the duties and requirements of an IRM, including continuing education. Unless otherwise designated, the college's Vice President of Information Technology will serve as the IRM.

The IRM will be assigned and designated these authorities:

1. a senior official within the organization,
2. reports directly to a person with a title functionally equivalent to the executive director or deputy executive director and
3. has been vested with the authority necessary to fulfill their duties as the Information Resources Manager.

Statutory IRM Responsibilities

Per the Information Resources Management Act, the IRM will:

1. oversee the Biennial Operation Plan (BOP) preparation, subject to instructions from the Legislative Budget Board (LBB);
2. provide input into the College's Strategic Plan;
3. comply with IRM continuing education requirements provided by DIR;
4. oversee the implementation of the organization's project management practices and
5. demonstrate in the organization's strategic plan the extent to which it uses its project management practices.

Other IRM Responsibilities

Other IRM responsibilities for this organization include

1. overseeing the acquisition and management of the organization's information resources;
2. reporting on the information resource (IR) investment and benefits to executive management, DIR, the Legislature, and the Legislative Budget Board;
3. adopting and executing IR standards, policies, practices, and procedures; and
4. complying with legislative mandates.

The IRM must have an educational background, experience, and qualifications provided by the Texas State Department of Information (DIR) resources. §211.21 (1)

The IRM shall complete continuing education programs, including educational materials and seminars, as provided by the Texas State DIR and approved by the board of the DIR. The President of Clarendon College is responsible for ensuring their appointed IRM remains qualified to serve as IRM. §211.21 (2)

The Clarendon College Information Security Officer (ISO) is designated the authority to oversee this policy.

The ISO will:

1. Perform periodic reviews to ensure compliance with this policy.
2. Notify the Information Resources Manager (IRM) of identified concerns and risks.

DEFINITIONS:

Data Access Review: The review and documentation of parties accessing data under the Data Owner's area of responsibility.

Data Custodian: The person responsible for overseeing and implementing physical, technical,

and procedural safeguards specified by the data owner.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Information Resources Manager (IRM): Officer responsible for the State of Texas managing Clarendon College's information technology resources.

Information Security Officer (ISO): Officer designated to administer the College Information Security Program.

Vice President of Information Technology: Has responsibilities for information systems operation; assisting in the installation and support of application software; network operations; installation, upgrade, and maintenance of network systems; installation, upgrade, and maintenance of all information technology; and user support and training.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Data Classification Policy:

PURPOSE:

Data Classification provides a framework for managing data assets based on value and associated risks and applying the appropriate levels of protection as required by state and federal law and proprietary, ethical, operational, and privacy considerations. All Clarendon College data, whether electronic or printed, must be classified as Confidential, Protected, or Public. Consistent use of data classification reinforces with users the expected level of protection of Clarendon College data assets under Clarendon College policies.

The purpose of the Data Classification Policy is to provide a foundation for developing and implementing necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

SCOPE:

The Clarendon College Data Classification policy applies equally to all Data Owners and Custodians.

POLICY STATEMENT:

Data Owners and/or Data Custodians must classify data as follows:

1. Confidential: Sensitive data must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act, FERPA, HIPPA) and other constitutional, statutory, judicial, and legal agreements. Examples of Confidential data may include, but are not limited to:
 - a. Personal Identifiable Information (PII) such as a name in combination with Social Security Number (SSN) and/or financial account numbers
 - b. Student education records, such as posting student identifiers and grades
 - c. Intellectual property such as copyrights, patents, and trade secrets
2. Medical records.
3. Protected: Sensitive data that may be subject to disclosure or release under the Texas Public Information Act but requires additional levels of protection. Examples of Protected data may include but are not limited to:
 - a. Operational information
 - b. Personnel records

- c. Information security procedures
- d. College-related research
- a. internal communications
- 4. Public: Information intended or required for public release as described in the Texas Public Information Act.

PII (Personally Identifiable Information) refers to any data that can be used to identify, contact, or locate an individual on its own or when combined with other information.

- 1. Examples of PII:
 - a. Direct Identifiers (can identify a person alone)
 - i. Full name
 - ii. Social Security Number (SSN)
 - iii. Driver's license number
 - iv. Passport number
 - v. Email address
 - vi. Phone number
 - b. Indirect Identifiers (can identify a person when combined with other data)
 - i. Date of birth
 - ii. IP address
 - iii. Employment records
 - iv. Physical address
 - v. Biometric data (fingerprints, retina scans)
 - c. Sensitive vs. Non-Sensitive PII
 - i. Sensitive PII: Requires extra protection (e.g., SSN, financial info, medical records).
 - ii. Non-Sensitive PII: Publicly available but can still be linked to a person (e.g., zip code, workplace).

Data Custodians will review annually the following for all data under their responsibility:

- 1. Data Classification: check to ensure data is correctly classified.
- 2. Data owner access and relevance.

DEFINITIONS:

Personally Identifiable Information (PII): Refers to any data that can be used to identify, contact, or locate an individual, either on its own or when combined with other information.

Confidential Data: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreement requirements).

Data Classification: Classifying data according to their Confidential, Protected, or Public category.

Data Custodian: The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place. See Appendix A for a listing of data owners.

Protected Data: Sensitive data that requires protection but may be subject to disclosure or release – Public Information Act.

Public Data: Information intended or required for public release.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix A

The following lists the various data categories and the respective data owners. Data includes all collected data and communications.

Data Category	Title of Data Owner
Admissions	Associate Dean of Admissions
Financial Aid	Director of Financial Aid
Accounting	Comptroller
Purchase Management	Accounts Payable Clerk
Human Resources	Benefits and Payroll Coordinator
Transcript/Grade Management	Registrar
Curriculum	Vice President of Academic Affairs
Contracts	Assistant to the President
Library Resources	Librarian
Work Force Education	Dean of CTE
Housing/Student Life	Vice President of Student Affairs
Athletics	Athletic Director
Facility Maintenance	Maintenance Supervisor
IT Services and Systems	Vice President of IT

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Data Backup and Recovery Policy:

PURPOSE:

The purpose of the Data Backup Policy is to manage and secure backup and restoration processes and the media employed within these processes; prevent the loss of data in the case of administrator error or corruption of data, system failure, or disaster; and ensure periodic restoration of data to confirm it is recoverable in a useable form.

SCOPE:

The Clarendon College Data Backup policy applies to any data owner, data custodian, system administrator, and Clarendon College-IT staff that installs, operates, or maintains Clarendon College information technology resources. Appendix A of this policy shows a schematic diagram of the backup process.

POLICY STATEMENT:

1. Clarendon College-IT System Administrators are responsible for backing up Clarendon College-IT-managed servers and must implement a tested and auditable process to facilitate recovery from data loss.
2. All departments should store data on the network rather than local storage (e.g., PC or Mac hard drive). Clarendon College-IT does not back up local storage and will be the data owner's responsibility.
3. Clarendon College-IT will perform timely data backups of all Clarendon College-IT-managed servers containing critical data for the abovementioned purposes.
 - a. Individual drives (redirected folders and mapped drives) and email will be retained for 90 days.
 - b. All other data, such as Enterprise Application Data (e.g., CAMS Enterprise, Dynamics GP, and SQL data) and shared storage backups, will be retained for 30 days.
 - c. Clarendon College will not be responsible for data stored on non-Clarendon College cloud storage systems (e.g., OneDrive), and data will be subject to that vendor's retention terms of service.
 - d. Cloud retention of all data backups is 30 days.
 - e. Learning Management System (LMS) backups are retained locally to the LMS for 30 days after the end of a term. They are then copied to the College's local server for retention for at least one year.
4. Determining which data and information is deemed 'critical' (e.g., confidential data and other data considered to be of institutional value) is the responsibility of the Data Owner under the Data Classification Policy. Data the Data Owner identifies as non-critical may be excluded from this policy.
 - a. Alternative backup schedules and media management may be requested by the data owner commensurate with the criticality of the data and the

- b. capabilities of the tools used for data storage.
5. Records retention is the responsibility of the Data Owner. The Clarendon College-IT backups are not to be used to satisfy the retention of records and are not customized for all the varying retention periods.
 6. Monthly backup data will be stored in a location that is physically different from the original data source.
 7. Verification must be performed regularly by restoring backed-up data as defined by the system's Clarendon College-IT backup procedures document.
 8. Procedures for backing up critical data and testing the procedures must be documented. Such procedures must include, at a minimum, for each type of data:
 - a. A definition of the specific data to be backed up.
 - b. The backup method (full backup, incremental backup, differential, mirror, or a combination).
 - c. The frequency and time of data backup.
 - d. The number of generations of backed-up data to be maintained (both on-site and off-site).
 - e. The responsible individual(s) for data backup.
 - f. The storage site(s) for the backups.
 - g. The storage media to be used.
 - h. The naming convention for the labels on storage media.
 - i. Any requirements concerning the data backup archives.
 - i. The data transport modes.
 - j. For data transferred during any backup process, end-to-end.
 - k. K. Security of the transmission path must be ensured for confidential data.
 - l. The recovery of backed-up data.
 - i. Processes must be maintained, reviewed, and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms.
 - m. The destruction of obsolete backup media as described in Clarendon College Media Sanitization Policy.

9. Backup Schedule

The following table represents the approved critical data, backup schedule, and data retention:

Server/Host	Data Description	Recovery Points	Local Retention	Offsite Retention	Offsite Replication
Server1	Accounting Database (GP/SQL)	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day
Server2	File shares	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day
Server3	AD / Security	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day
Server4	Terminal Server	Hourly 24-hrs day	30 Rolling Days	3 Rolling Days	Update from 1 AM Nightly / SC Cloud to Hourly 24-hrs day

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Cloud Storage: A service model in which data is maintained, managed, backed up remotely, and made available to users over the Internet.

Incremental Backup: A backup containing only the files that have changed since the most recent backup (either full or incremental). The advantage of this is quicker backup times, as only changed files need to be saved. The disadvantage is longer recovery times, as the latest full backup and all incremental backups up to the date of data loss need to be restored.

Full Backup: A backup of all (selected) files on the system. In contrast to a drive image, this does not include the file allocation tables, partition structure, and boot sectors.

Disk Image: Single file or storage device containing the complete contents and structure representing a data storage medium or device, such as a hard drive, tape drive, floppy disk, CD/DVD/BD, or USB flash drive.

Site-to-Site Backup: Backup, over the internet, to an offsite location under the user's control. It is similar to remote backup, except that the data owner maintains control of the storage location.

Related Policies, References and Attachments:

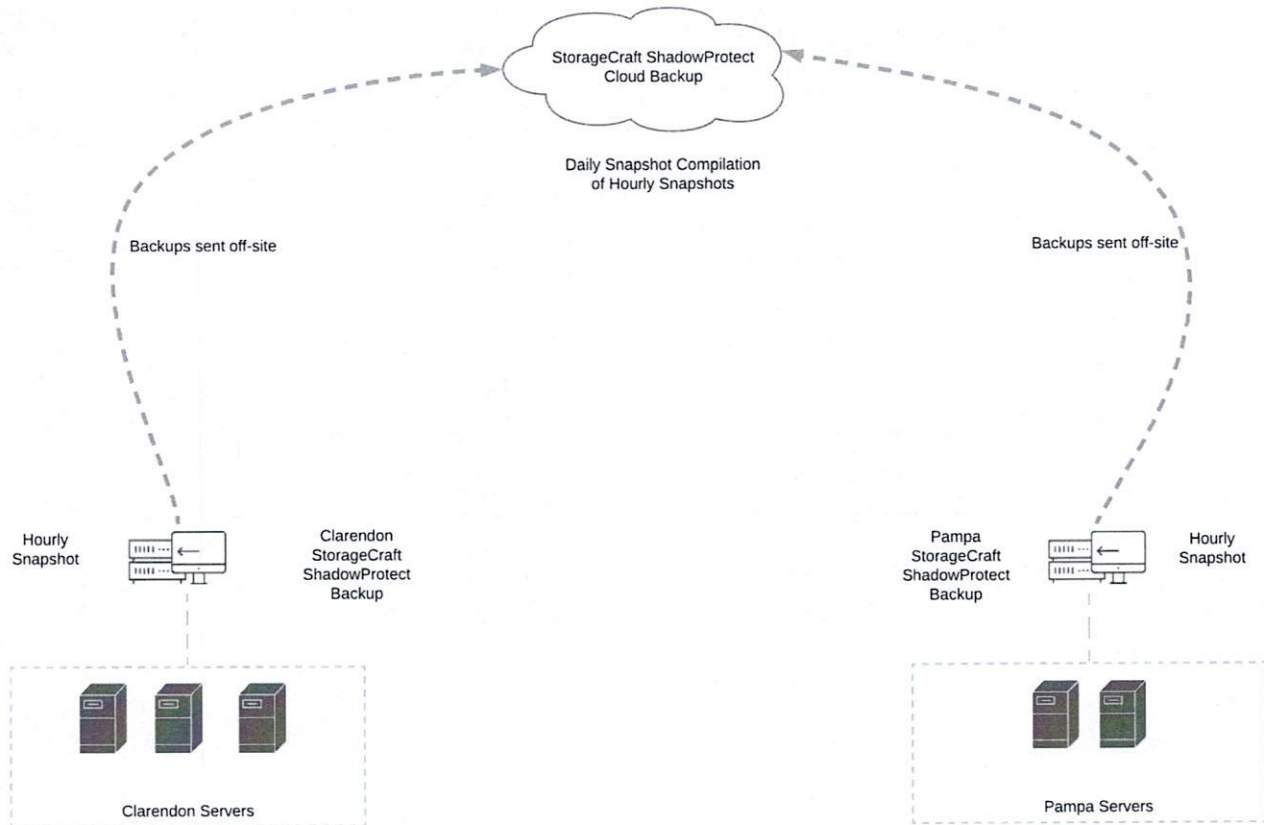
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix A

The diagram below depicts a schematic diagram of the Clarendon College backup system.



The Clarendon College Board of Regents approved this policy on _____, version 1.2.
This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix B: Identification of Critical Applications

The following is a list of critical software and data for Clarendon College and its importance to date-to-date operations and backup disposition.

Importance	Application Name	Data Type	Business Impact	Backup	Sys Location	Backup Location
1	Server Systems	Virtual Server Instances	Very Critical	Yes	On-Site	On-Site/Cloud
1	CAMS Enterprise	Student Information System	Very Critical	Yes	On-Site	On-Site/Cloud
2	ED Express	Financial Aid	Critical	Yes, Data Only	On-Site	On-Site/Cloud
2	ED Connect	Financial Aid	Critical	Yes, Data Only	On Site	On Site/Cloud
3	OpenLMS	Learning Management System	Critical	Yes	Cloud	On Site/Cloud
3	Dynamics GP	Accounting	Critical	Yes	On Site	On Site/Cloud
3	Pearson Vue	Testing	Critical	Yes	On Site	On Site
4	Shared Folders	Various	Critical	Yes	On Site	On Site/Cloud
4	User Directories	Various	Critical	Yes	On Site	On Site/Cloud
5	Microsoft Office	Various	Critical	No	On Site	N/A
6	Other User Apps	Various	Moderate	No	On Site	N/A

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2023.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Digital Encryption Policy:

INTRODUCTION:

Clarendon College complies with state and federal statutes that protect confidential information.

Information technology resources that contain or transmit confidential information must be protected with the specified minimum requirements for encryption key standards and management.

SCOPE:

The Clarendon College Digital Encryption Policy applies equally to all individuals entrusted with any Clarendon College information technology resources.

POLICY STATEMENT:

Minimum encryption requirements to protect confidential information from unauthorized disclosure shall be limited to the following State of Texas encryption requirements:

1. Public information, described in the Texas Public Information Act or other enabling laws, rules, and regulations, has no minimum encryption requirements.
2. Confidential information must be protected from unauthorized disclosure or public release based on state or federal law, and personal identifying or sensitive personal information, as defined in the Texas Business and Commerce Code, must be encrypted with a minimum of 128-bit key length. The preferred key length is AES 256-bit length.
3. Federally protected data, federal tax information, protected health information, and law enforcement information must comply with NIST certification to FIPS 140-3 (Security Requirements for Cryptographic Modules) standards or the current standard.

Confidential information transmitted through or stored in an externally accessible location shall be encrypted from when it leaves a secure location until it is received in a safe location.

Confidential information should not be copied to or stored on removable media or a non-agency-owned computing device that is not encrypted.

Clarendon College may also implement these protections for data classifications other than Confidential.

Information resources assigned from one state agency to another or from a state agency to a contractor or other third-party representative shall be protected by the conditions imposed by the providing state agency.

DEFINITION:

Data Encryption: Data encryption translates data into another form or code so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is called ciphertext, while unencrypted data is called plaintext.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at

<https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Email Usage Policy:

PURPOSE:

To prevent tarnishing the public image of Clarendon College and provide a safe and secure communication system. When an email goes out from Clarendon College, the general public may view that message as an official statement from Clarendon College.

This policy covers the appropriate use of any email sent from a Clarendon College email address and applies to all employees, students, vendors, and agents operating on behalf of Clarendon College.

This document establishes specific requirements for using all computing and network resources at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202) and Texas Higher Education Coordinating Board)

SCOPE:

The Clarendon College Acceptable Use Policy applies equally to all individuals utilizing Clarendon College information technology resources (e.g., employees, faculty, students, retirees, agents, consultants, contractors, volunteers, vendors, temps, etc.).

Information technology resources include all College-owned, licensed, or managed hardware and software and use of the College network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

RIGHTS AND RESPONSIBILITIES:

As college community members, users are provided with scholarly and/or work-related tools, including access to the library, specific computer systems, servers, software, databases, campus telephone and voice mail systems, and the Internet. There is a reasonable expectation of unobstructed use of these tools, certain degrees of privacy (which may vary depending on whether the user is a College employee or a registered student), and protection from abuse and intrusion by others sharing these resources.

In turn, users are responsible for knowing the regulations and policies of the College that apply to the appropriate use of the College's technologies and resources. Users are responsible for exercising good judgment when using the college's technological and information resources. Just because an action is technically possible does not mean it is appropriate to perform it.

Users are representatives of the Clarendon College community and are expected to respect the College's good name in electronic dealings with those outside the College.

1. Responsibility of the Sender:

- a. Ensure that emails are sent to the correct recipients.

- b. Clearly state the purpose of the email in the subject line.
- c. Provide all necessary information and attachments.
- d. Follow up on essential emails if no response is received within a reasonable timeframe.

2. Responsibility of the Recipient:

- a. Regularly check and read emails.
- b. Respond to emails promptly.
- c. Notify the sender if an email has been received in error.
- d. Ensure that email notifications are enabled and functioning.

3. Accountability:

- a. The sender is not responsible for any consequences arising from the recipient's failure to check or respond to their email.
- b. The recipient is accountable for staying informed about communications sent to their email address.

PRIVACY:

All users of College networks and systems should remember that all usage of information technology resources can be recorded and is the property of Clarendon College. Such information is subject to the Texas Public Information Act and the laws applicable to college records retention. Employees have no right to privacy concerning the use of college-owned resources. Clarendon College management has the ability and right to view employees' usage patterns and act to ensure that College resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on Clarendon College information technology resources owned, leased, administered, or otherwise under the custody and control of Clarendon College are not private. They may be accessed by appropriate personnel following the provisions and safeguards provided in the Texas Administrative Code 1 TAC§202 (Information Security Standards).

ACCEPTABLE USE:

The Clarendon College network supports research, education, and administrative activities by providing access to computing resources and collaborative work opportunities. Primary use of the Clarendon College network must be consistent with this purpose.

Access to the Clarendon College network from any device must adhere to all the same policies that apply to use from within Clarendon College facilities.

1. All employees will receive an email account.
2. Users may use only Clarendon College information technology resources for which they are authorized.
3. Users are individually responsible for appropriately using all resources, including the computer, the network address or port, software, and hardware. They are accountable to the College for all use of such resources.
4. Authorized users of Clarendon College resources may not enable unauthorized users to

access the network. The College is bound by its contractual and license agreements respecting specific third-party resources; users must comply with all such agreements when using Clarendon College information technology resources.

5. Users should secure resources against unauthorized use or access, including Clarendon College accounts, passwords, Personal Identification Numbers (PINs), Security Tokens (i.e., smartcards), or similar information or devices used for identification and authorization purposes.
6. Users must report shareware or freeware before installing it on Clarendon College-owned equipment unless it is on the approved software list. A request to install software must be reported to the Clarendon College-IT via email before installing any software.
7. Users must not attempt to access Clarendon College information technology resources without appropriate authorization by the system owner or administrator.
8. Email is an official means of communication within Clarendon College. Therefore, the College has the right to send communications to faculty, staff, and students via email and the right to expect that those communications will be received and read in a timely fashion. If you have an Internet Service Provider, you can access the College's email system from on-campus and off-campus.
9. Faculty, staff, and students must check their official email addresses frequently and consistently to stay current with College communications. The College recommends checking email at least once a day in recognition that certain communications may be time-critical.
10. An email account will be removed upon notice of termination from Human Resources unless the Benefits & Payroll Coordinator requests an extension. An extension can either be 30 days, in cases where departments need the ability to transfer information, or on further notice, if the person involved will have an ongoing relationship with Clarendon College.
11. Adhere to the Clarendon College Communications Policy.

RESTRICTIONS:

All individuals are accountable for their actions relating to Clarendon College's information technology resources. Direct violations include the following:

1. Interfering or altering the integrity of Clarendon College information technology resources by:
 - a. Impersonating other individuals in communication;
 - b. Attempting to capture or crack passwords or encryption;
 - c. Unauthorized access, destruction, or alteration of data or programs belonging to other users;
 - d. Excessive use for personal purposes, meaning use that exceeds incidental use as determined by supervisor; or,
 - e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws.

2. Allowing family members or unauthorized persons to access Clarendon College's information technology resources.
3. Sending Personally Identifiable Information (PII) via an unencrypted or unsecured email is forbidden. The use of secure/encrypting processes is a must when sending any email that contains PII information.
4. Using the Clarendon College information technology resources for private financial gain or personal benefit. Users cannot run private businesses on Clarendon College's information technology resources. Commercial activity is permitted but only for business done on behalf of Clarendon College or its organizations.
5. Activities that would jeopardize the College's tax-exempt status.
6. Using Clarendon College information technology resources for political gain.
7. Using Clarendon College information technology resources to threaten or harass others violating College policies.
8. Intentionally accessing, creating, storing, or transmitting material that Clarendon College may deem to be offensive, indecent, or obscene (other than in the course of academic research or authorized administrative duties where this aspect of the study or work has the explicit approval of the Clarendon College official processes for dealing with academic ethical issues).
9. Not reporting any weaknesses in Clarendon College information technology resources security or any incidents of possible misuse or violation of this agreement by contacting the Information Security Officer.
10. Attempting to access any data or programs on Clarendon College information technology resources for which authorization has not been given.
11. Redirection or automatic email forwarding of the college's email system to a personal email system by college employees is forbidden.
12. Making unauthorized copies of copyrighted or licensed material.
13. Intentionally using or attempting to introduce worms, viruses, Trojan horses, or other malicious code onto a Clarendon College information resource.
14. Degrading the performance of Clarendon College information technology services; depriving an authorized Clarendon College user access to a Clarendon College information technology resource; obtaining extra information technology resources beyond those allocated; or circumventing Clarendon College security measures.
15. Downloading, installing, or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Clarendon College users must not run password-cracking programs, packet sniffers, port scanners, or any other non-approved programs on Clarendon College information technology services.
16. Engaging in acts against the aims and purposes of Clarendon College as specified in its governing documents or rules, regulations, and procedures adopted by Clarendon College, Texas Department of Information Resources (TAC 202), and the Texas Higher Education Coordination Board.
17. Allowing another person, either through one's computer account or other means, to accomplish any of the above.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Computer Virus: A type of malicious software program ("malware") that, when executed, replicates by reproducing itself (copying its source code) or infecting other computer programs by modifying them.

Copyright Laws: A form of protection provided by the laws of the United States to authors of "original works of authorship." This includes literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations.

Freeware: Software that is available for use at no monetary cost.

Information Security Officer (ISO): Officer designated to administer the College Information Security Program.

Malicious Code: A term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

Shareware: A type of proprietary software initially provided free of charge to users, who are allowed and encouraged to make and share copies of the program.

Encrypted Email: This message has been scrambled to prevent unauthorized access. It's a security measure that protects sensitive information from being read by cybercriminals.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Firewall Policy:

PURPOSE:

The Clarendon College gateways are protected by external firewalls between the Internet and the Clarendon College network to establish a secure environment for the College's information technology resources. Internal firewalls are in place to establish secure communications between different segments of the College's network where various levels of security are warranted. Firewalls are enabled and configured on servers and workstations attached to the college's internal network.

Clarendon College's firewalls are key components of the College's network security architecture. The Firewall Policy governs how firewalls filter traffic to mitigate the risks and losses associated with security threats to Clarendon College's information technology resources. This policy will attempt to balance risks incurred against the need for access.

This policy aims to protect Clarendon College's information technology resources from hacking and virus attacks by restricting access to information technology resources on the College campus. It is designed to minimize the potential exposure of Clarendon College to the loss of sensitive, confidential data, intellectual property, and damage to the public image, which may follow from unauthorized use of Clarendon College's information technology resources.

SCOPE:

The Firewall Policy applies to all firewall devices owned and/or operated by Clarendon College.

POLICY STATEMENT:

Perimeter Firewalls:

The perimeter firewall permits the following outbound and inbound Internet traffic:

1. *Outbound* - All Internet traffic to hosts and services outside Clarendon College's networks except those specifically identified and blocked as malicious sites.
2. *Inbound* - Allow Internet traffic that supports the institution's mission by defining system, application, and service procedures.
3. *Outbound/Inbound* - All internet traffic detected as malicious by the College's intrusion prevention system (IPS) and/or all traffic violating Clarendon College firewall policies is dropped.

Reason for filtering ports:

1. Protecting Clarendon College Internet Users - Certain ports are filtered to protect Clarendon College's information technology resources. The perimeter firewall protects against certain common worms and dangerous services on Clarendon College information technology resources that could allow intruders access.

2. Protecting our outbound bandwidth - If Clarendon College Internet users overuse their outbound bandwidth by running high-traffic servers or by becoming infected with a worm or virus, it can degrade the service of other Clarendon College systems.
3. Protecting the rest of the Internet - Some filters prevent users from knowingly or unknowingly attacking other computers. In addition to being in Clarendon College's interest in protecting our bandwidth, it is the institution's responsibility to prevent abuse of its network.

Roles and Responsibilities:

The Information Security Office is responsible for implementing, configuring, and maintaining Clarendon College's firewalls and activities relating to this policy.

1. At a minimum, firewalls must be annually tested and reviewed.
2. When there are significant changes to the network requirements, firewall security policies will be reviewed and may warrant changes.
3. Firewalls must have alert capabilities and supporting procedures.
4. Auditing must be active to permit analysis of firewall activity.
5. All firewall changes will be documented.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Firewall: This is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Gateway: This is the computer or device that routes the traffic from a workstation to the outside network serving the Web pages.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Identification/Authentication Policy:

PURPOSE:

The Identification/Authentication Policy aims to ensure the security and integrity of Clarendon College data and information technology resources by ensuring controls for securing user identification and authentication credentials.

To ensure the security and integrity of Clarendon College data, identified users will securely authenticate to Clarendon College information technology resources and access only resources they have been authorized to access.

If user identities are not properly authenticated, Clarendon College has no assurance that access to information technology resources is adequately controlled. This policy will mitigate the risk of unauthorized access to information and establish user accountability and rules for access.

SCOPE:

The Identification/Authentication Policy applies to all individuals granted access to Clarendon College information technology resources.

POLICY STATEMENT:

Clarendon College shall require that systems are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication (any or all of the basic authentication methods), and implementing access controls on Clarendon College's information technology resources. Access control is provided at the firewall, network, operating system, and application levels.

Clarendon College managers/supervisors are responsible for requesting access to information systems, approving user access privileges based on their assigned duties, and notifying Data Owners and Clarendon College-IT of the termination of access to information technology resources.

Before being granted access to Clarendon College information technology resources, the needs of the employee, student worker, contractor, vendor, guest, or volunteer shall be given ample consideration, and authorization granted to allow access to Clarendon College information technology resources, access should be granted according to the principle of least privilege as outlined in IT Administrator/Special Access Policy.

Clarendon College accounts will have a unique identifier associated with a single user. Once an identifier is assigned to a particular person, it is always associated with that person. It is never subsequently reassigned to identify another person.

Using the authentication service to identify oneself to a Clarendon College system constitutes an official identification of the user to the College, in the same way that presenting an ID card does. Security is everyone's responsibility, and everyone must protect their "identity." Users will be held accountable for all actions of their accounts.

Regardless of the authentication method used, users must use only the authentication information they have been authorized to use; i.e., they must never falsely identify themselves as another person. Additionally, users must keep their authentication information confidential; i.e., they must not knowingly or negligently make it available for use by an unauthorized person. Anyone suspecting their authentication information has been compromised should contact the Information Security Officer immediately.

Users must adhere to the Clarendon College User Accounts Password Policy requirements.

Clarendon College Data Owners shall ensure that authorization and account management processes are documented and that the appropriate people have been responsible for creating and maintaining authorization records.

Clarendon College Data Owners may monitor individuals' related activities as a condition for continued access. At a minimum, Clarendon College Data Owners must review user access privileges annually.

DEFINITIONS:

Authentication Credentials: The verification of the identity of a user who wishes to access a system, commonly using a password in conjunction with a unique UserID.

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks to minimize the potential impact of a threat.

Principle of Least Privilege: Limiting computer user profile privileges to only the necessary information and resources based on users' job necessities.

Unauthorized Access: Access by a person without official permission or approval to access Clarendon College systems.

User Identification: A unique sequence of characters to identify a user and allow access to a computer system or network.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on July 15, 2023.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Intrusion Detection/Prevention and Security Monitoring Policy:

PURPOSE:

The Clarendon College Information Security Officer is charged with securing all Clarendon College-owned information technology resources, both centralized and decentralized, and has the responsibility and College-wide authority to monitor the use of information technology resources to confirm that security practices and controls are in place, are effective and are not being bypassed.

The purpose of the Intrusion Detection/Prevention and Security Monitoring Policy is to outline College policy regarding the monitoring, logging, and retention of network packets that traverse Clarendon College networks, as well as observe events to identify problems with security policies, document existing threats and evaluate/prevent attacks.

Intrusion Detection and Prevention systems identify possible incidents, log information about them, and report attempts to security administrators. It plays a vital role in implementing and enforcing security policies.

Clarendon College takes reasonable measures to assure the integrity of private and confidential electronic information transported over its networks and to detect attempts to bypass the security mechanisms of information resources. This will allow for early detection of wrongdoing, new security vulnerabilities, or new unforeseen threats to information technology resources, thus minimizing the potentially harmful impact.

Protecting sensitive information and mitigating risks to the college's network infrastructure is paramount for several reasons:

1. **Preservation of Privacy:** Students, faculty, staff, and other stakeholders entrust the college with their personal and sensitive information. Safeguarding this data is essential for preserving their privacy and maintaining trust in the institution.
2. **Legal Compliance:** The college is subject to various laws and regulations governing the protection of sensitive information, such as the Family Educational Rights and Privacy Act (FERPA) in the United States. Failure to comply with these regulations can result in legal penalties, financial liabilities, and damage to the college's reputation.
3. **Intellectual Property Protection:** The college can often possess valuable intellectual property, including research data, proprietary software, and innovative ideas developed by faculty and students. Protecting this intellectual property from unauthorized access, theft, or tampering is critical for maintaining the institution's competitiveness and fostering a culture of innovation.

4. **Continuity of Operations:** Disruptions to the college's network infrastructure, whether due to cyberattacks, data breaches, or other security incidents, can disrupt normal operations, compromise academic activities, and impede the delivery of essential services. Mitigating risks to the network infrastructure helps ensure the continuity of operations and minimizes the impact of potential disruptions.
5. **Financial Stability:** Security incidents can have significant financial implications for the college, including remediation costs, legal expenses, regulatory fines, and loss of revenue or funding. By proactively protecting sensitive information and mitigating risks to the network infrastructure, colleges can avoid costly security breaches and preserve their financial stability.
6. **Reputation Management:** Clarendon College relies on its reputation to attract students, faculty, donors, and other stakeholders. A security breach or data leak can tarnish the college's reputation, erode stakeholder trust, and undermine its standing within the academic community. Protecting sensitive information and maintaining a secure network infrastructure are essential for the college's reputation and credibility.

Overall, protecting sensitive information and mitigating risks to the college's network infrastructure is essential for ensuring compliance with regulations, preserving privacy, maintaining continuity of operations, safeguarding intellectual property, preserving financial stability, and protecting the institution's reputation. Colleges can effectively manage these risks by prioritizing security measures, investing in robust cybersecurity practices, and safeguarding their assets and stakeholders.

SCOPE:

The Intrusion Detection/Prevention and Security Monitoring Policy applies to all individuals responsible for installing new information technology resources, operating existing information technology resources, and individuals charged with information technology resource security. Furthermore, this policy applies to all Clarendon College's network resource users, including students, faculty, staff, and third-party contractors.

POLICY STATEMENT:

Clarendon College considers all electronic information transported over the College network to have the potential to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as such.

While it is not the policy of Clarendon College to actively monitor internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the college's internet links. Any inspection of electronic data packets and any action performed following such inspection will be governed by all applicable federal and state statutes and Clarendon College policies. Additionally, the college is committed to respecting user privacy while monitoring network activity, and any or all monitoring will occur only when necessary under applicable laws and policies.

Please refer to the Clarendon College Technology Incident Management Policy for reporting suspected or confirmed instances of intrusions or attempted intrusions.

Audit logging, alarms, and alert functions of operating systems, user accounting, application software, firewalls, and other network perimeter access control systems will be enabled and reviewed annually. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually; see the Clarendon College Firewall Policy. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Information Security Officer.

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. A security baseline will be developed where possible, and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- Local Area Network (LAN) traffic, protocols, and device inventory
- Operating system security parameters

The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Service desk trouble tickets and telephone call logs
- Network printer logs

Log checks and data monitoring will be reviewed quarterly depending on the risk profile of the college's network environment.

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Operating system and software licenses

Any security issues discovered will be reported immediately to the Information Security Officer (ISO).

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Project Lifecycle Policy:

PURPOSE:

This policy establishes guidelines for managing the lifecycle of Information Technology (IT) projects at Clarendon College. It ensures IT investments align with institutional goals, comply with regulations, and provide sustainable, secure, and efficient solutions.

SCOPE:

This policy applies to all IT projects undertaken by the college, including hardware, software, network infrastructure, and cloud-based solutions.

POLICY STATEMENT:

1. IT Project Lifecycle Phases

Initiation

- a. Define project objectives, scope, and stakeholders.
- b. Conduct feasibility analysis and risk assessment.
- c. Secure approval from the IT Governance Committee.
- d. Identify funding sources and budget requirements.

Planning

- a. Develop a detailed project plan, including timeline, milestones, and resource allocation.
- b. Conduct stakeholder engagement and requirement analysis.
- c. Define key performance indicators (KPIs) for success measurement.

Development & Implementation

- a. Procure necessary hardware, software, and services.
- b. Configure, develop, and integrate systems per requirements.
- c. Conduct security, compliance, and accessibility assessments.
- d. Perform testing, user training, and documentation.

Maintenance & Support

- a. Establish a support structure for troubleshooting and updates.
- b. Implement regular security and performance assessments.
- c. Provide ongoing training and user support.
- d. Monitor KPIs and adjust as necessary.

Retirement & Decommissioning

- a. Develop an end-of-life transition plan.
- b. Migrate or archive critical data following retention policies.
- c. Decommission outdated systems securely and environmentally responsibly.
- d. Conduct a post-project evaluation and document lessons learned.

2. Roles and Responsibilities

- a. **IT Governance Committee:** Approves and prioritizes projects.
- b. **Project Manager:** Oversees execution and ensures compliance with the policy.
- c. **IT Security Team:** Ensures adherence to cybersecurity standards.

d. **Stakeholders:** Provide input, feedback, and validation throughout the lifecycle.

3. Compliance & Review

- a. All IT projects must adhere to federal, state, and institutional regulations.
- b. This policy will be reviewed annually and updated as needed.

4. Exceptions

Exceptions to this policy require written approval from the Vice President of Information Technology and justification outlining the necessity of the deviation; see Compliance Policy and the Policy Exemption Form.

DEFINITIONS:

IT Governance Committee: A group that oversees an organization's IT strategy, systems, financing, and risk management. The committee's role is to ensure the organization's IT investments align with its goals. A committee consisting of the President, Vice President of Academic Affairs, and the Vice President of Information Technology.

Key Performance Indicator (KPI) IT Lifecycle: Refers to the complete process of identifying, selecting, implementing, monitoring, and refining key metrics that measure the performance of an IT system or service throughout its lifecycle, allowing organizations to track progress towards their strategic goals and identify areas for improvement within their IT operations.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Malicious Code Policy:

PURPOSE:

This policy is intended to provide information to College information technology resource administrators and users to improve the resistance to, detection of, and recovery from the effects of malicious code.

Clarendon College information technology resources are strategic assets that must be managed as valuable College resources. The integrity and continued operation of College information technology resources are critical to the operation of the College. Malicious code can disrupt the regular operation of College information technology resources.

The number of information technology resource security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents can reduce the risk and decrease the cost of security incidents.

SCOPE:

The Clarendon College Malicious Code Policy applies equally to all individuals utilizing Clarendon College information technology resources (e.g., employees, faculty, students, retirees, agents, consultants, contractors, volunteers, vendors, temps, etc.).

This policy does not apply to approved faculty research and academic programs where students and instructors develop and experiment with malicious programs in a controlled environment.

POLICY STATEMENT:

The following requirements shall be adhered to at all times to ensure the protection of Clarendon College information technology resources:

Prevention and Detection:

1. All desktops and laptops connected to the Clarendon College network must use Clarendon College-approved virus protection software and configuration.
2. Each file server attached to the Clarendon College network must utilize Clarendon College-approved virus protection software and be set up to detect and clean viruses that may infect file shares.

3. Software to safeguard against malicious code (e.g., antivirus, anti-spyware, etc.) shall be installed and functioning on susceptible information technology resources with access to the College network.
4. All information technology resource users are prohibited from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.) unless they are part of an approved research or academic program.
5. All information technology resource users are prohibited from knowingly propagating malicious programs, including opening attachments from unknown sources.
6. Email attachments and shared files of unknown integrity shall be scanned for malicious code before they are opened or accessed.
7. Flash drives, external hard drives, and other mass storage devices will be scanned for malicious code before accessing any data on the media.
8. Software safeguarding information technology resources against malicious code should not be disabled or bypassed by end-users.
9. The settings for software that protect information technology resources against malicious code should not be altered to reduce the software's effectiveness.
10. The automatic update frequency of software that safeguards against malicious code should not be turned off, altered, or bypassed by end-users to reduce the frequency of updates.

Response and Recovery:

1. Upon discovering a suspected malicious code, the IT department or any vendor working on behalf of the IT department must be notified as soon as possible.
2. All reasonable efforts shall be made to contain the effects of any system infected with a virus or malicious code. This may include disconnecting systems from the network or disabling service.
3. If malicious code is discovered or believed to exist, an attempt should be made to remove or quarantine the malicious code using current antivirus or other control software.
4. If malicious code cannot be automatically quarantined or removed by antivirus software, the system should be disconnected from the network to prevent further propagation of the malicious code or other harmful impact. The presence of the malicious code shall be reported to the Clarendon College IT Department.
5. Personnel responding to an incident should be given access privileges and authority to afford the necessary measures to contain/remove the infection.
6. If possible, identify the source of the infection and the type of infection to prevent recurrence.

7. Any removable media (including flash drives, external hard drives, mass storage cards, etc.) recently used on an infected machine shall be scanned before opening and/or executing any files.
8. Clarendon College-IT personnel or any vendor working on behalf of the Clarendon College IT department should thoroughly document the incident, noting the source of the malicious code (if possible), resources impacted, and damage or disruption to information technology resources, and submit to the Information Security Officer to be included in the Department of Information Resources Security Incident Reporting System.
9. Refer to the Intrusion Detection/Prevention and Security Monitory Policy for logging and recording any reported malicious code.

DEFINITIONS:

Clarendon College IT: The department or any vendor working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Information Security Officer (ISO): Officer designated to administer the College Information Security Program.

Malicious Code: A term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks to minimize the potential impact of a threat.

Security Incident: A single event or a series of unwanted or unexpected events that involve information security (see definition of "information security event"), causing harm or threatening information assets and requiring non-routine preventative or corrective action.

Virus Protection Software: Software designed to prevent viruses, worms, and Trojan horses from getting onto a computer, as well as remove any malicious code that has already infected a computer.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Media Sanitization Policy:

PURPOSE:

Clarendon College's policy is that all data must be removed from devices and equipment capable of data storage, transmission, or receipt before equipment disposal.

The technical support staff will properly sanitize information technology resources before transferring, selling, or disposing. All devices capable of storing Clarendon College information must be sanitized in a way that will make data recovery impossible.

This document establishes specific requirements for Information Technology media sanitization at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202))

SCOPE:

The Clarendon College Media Sanitization Policy applies to any data owner, data custodian, system administrator, and Clarendon College-IT staff that installs, operates, or maintains Clarendon College information technology resources.

POLICY STATEMENT:

Before the sale, transfer, or disposal of information technology resources, the technical support staff will take the appropriate steps, per the Clarendon College-IT Media Sanitization Procedures, to remove all data from any associated storage device.

1. Information technology resources shall be sanitized utilizing a method that will ensure data recovery is impossible, such as degaussing, shredding, or destroying the media using a destruction method that will be able to withstand a laboratory attack (e.g., disintegration, pulverization, melting or incineration).
2. If the device is a cell phone or handheld electronic device, remove the subscriber identity module (SIM) and additional memory cards and destroy them per sanitization requirements. Sanitize the unit utilizing a method that will ensure data recovery is impossible.
3. Document the removal and completion of the process with the following information:
 - a. Date;
 - b. Description of the item(s) and serial number(s);
 - c. Inventory number(s);
 - d. The process and sanitization tools used to remove the data, or process and method used for destruction of the media; and
 - e. The name and address of the organization to which the equipment was transferred, if applicable.

4. Remove the asset from the Clarendon College IT and equipment inventory. Ensure the removal of the asset by providing the information from item 3 to the Clarendon College Comptroller.
5. All steps above will also be followed when the asset(s) are sold to a third party for resale or destruction.

DEFINITION:

Subscriber Identity Module (SIM): This is an integrated circuit (IC) intended to securely store an international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephone devices (such as mobile phones and laptops). SIMs can also store address book contact information and may be protected using a PIN code to prevent unauthorized use.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Non-Disclosure Agreement Policy:

PURPOSE:

Non-disclosure agreements are contracts intended to protect information considered to be sensitive or confidential. Information technology resources shall be used only for intended purposes as defined by Clarendon College (Clarendon College) and in compliance with applicable laws.

All individuals are accountable for their actions relating to information technology resources. They shall formally acknowledge that they will comply with the Clarendon College security policies and procedures or will not be granted access to information technology resources. All employees will complete a non-disclosure agreement for information technology resources annually.

This document establishes specific requirements for Non-Disclosure Agreements at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202) and Texas Administrative Code, Title 1, Part 10, Chapter 203, Subchapter B (TAC§203))

SCOPE:

The Non-Disclosure Agreement Policy applies to all authorized users who utilize Clarendon College's information technology resources (including, but not limited to, Clarendon College Faculty, staff, student workers, temporary employees, vendors, consultants, employees of independent contractors, and personnel from other schools.)

POLICY STATEMENT:

All users must sign the Clarendon College Non-Disclosure Agreement (NDA), acknowledging they have read and understand Clarendon College requirements regarding computer security policies and procedures. A copy of the Clarendon College Information Security Users Guide will be sent along with the NDA. This signed non-disclosure agreement becomes a permanent record and will be renewed annually.

Electronic signatures are an acceptable means of acknowledging Clarendon College's Non-Disclosure Agreement.

DEFINITIONS:

Non-Disclosure Agreement (NDA): Formal acknowledgment that all employees must sign, acknowledging they have read and understand Clarendon College's computer security policies and procedures requirements. This agreement becomes a permanent record and will be renewed annually.

Electronic Signature: The digital equivalent of a handwritten signature offers far more inherent security, which provides the added assurance of evidence of acknowledging informed consent by the signer.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Network Use and Vulnerability Assessment Policy:

PURPOSE:

The Network Use and Vulnerability Assessment policy aims to assure the telecommunications network infrastructure's reliability, security, integrity, and availability. This policy documents practices and responsibilities associated with the administration, maintenance, expansion, and use of the College network to:

1. Provide reliable network communications for the efficient conduct of College business;
2. Assure that network usage is authorized and consistent with the College's mission and
3. Protect the confidentiality, integrity, and availability of College information that traverses the College network.

SCOPE:

The Clarendon College Network Use and Vulnerability Assessment policy applies equally to all individuals utilizing any Clarendon College information technology resources.

POLICY STATEMENT:

The Information Resources Manager (IRM) has central oversight and manages the Clarendon College network infrastructure resources. All devices connected to the Clarendon College network (wired or wireless) should support the College's mission. The integrity, security, and proper operation of the College network require an orderly assignment of network addresses and attached device configuration. Network access, performance, and security are at risk when devices are introduced into the network environment without appropriate coordination.

Clarendon College-IT will perform periodic vulnerability assessments and network scans to determine if assets hosted on Clarendon College's network are vulnerable to any known flaws in the operating system, services, or application. The results are intended to assist server and application owners in securing their assets and any College-related data they may house. Server or Application owners will be notified of any vulnerability present on their systems, and any servers whose vulnerabilities have not been remediated in a predetermined amount of time may be disconnected from Clarendon College's network.

Clarendon College-IT manages College network connections with consideration for the College mission, accessibility, performance, privacy, and security in compliance with the following:

1. No individual or College component may independently deploy network devices that extend the College network or secure or isolate parts of the College network except as stipulated under this policy's provisions.

2. Clarendon College-IT is responsible for adequately deploying and managing a fully monitored and protected network communication service, including all infrastructure elements, network address assignments, and radio frequency (RF) spectrum usage.
3. Clarendon College-IT shall coordinate the connection and network address assignment of any devices on the College network. Other departments and individual users may not install, alter, extend, or re-transmit network services in any way without prior proper approval.
4. Departments and individual users are prohibited from attaching or contracting with a vendor to attach port-assignable, hard-wired equipment such as routers, switches, hubs, firewall appliances, wireless access points, virtual private network (VPN) servers, network address translators, proxy servers, and dial-up servers to the College network without prior authorization from Clarendon College-IT.
5. Clarendon College-IT may disconnect and remove any Clarendon College-IT unauthorized network device, including wireless routers and access points.
6. Personal software firewalls are permitted, as are printers, scanners, and similar peripheral devices if directly connected as a peripheral device to a desktop or notebook computer. Clarendon College-IT must approve any such device. Clarendon College-IT reserves the right to monitor and audit individual devices, systems, and general network traffic to ensure compliance with this and other College policies.
7. Certain responsibilities accompany using devices connected to the College network. Specifically, all users must ensure timely updates of applications, operating systems, and virus protection software to minimize risks of system compromise. (Clarendon College-IT provides non-intrusive products and services to achieve such updates.)
8. The College network is unencrypted. Server and application administrators that utilize this network to transmit sensitive, restricted, and confidential information are responsible for information security. Examples of available protections include encrypted protocols such as SSL, IPsec, SSH, etc. Contact Clarendon College-IT for assistance in implementing the necessary protective measures.
9. Clarendon College-IT requires the registration of servers connected to the College network, which must be collocated in the Clarendon College-IT data center. Following registration, Clarendon College-IT will facilitate an information-technology risk assessment to ensure compliance with state and College standards and best practices. A department's administrative head is responsible for designating a server administrator for each server. The server administrator shall collaborate with Clarendon College-IT as necessary to:
 - a. Register the server with the ISO;
 - b. Protect the server against exploitation of known vulnerabilities.
 - c. Address and resolve security problems identified with any device or application they are responsible for.
 - d. Utilize the protection benefits available through the College's network edge protection mechanisms (e.g., firewall, intrusion prevention systems, etc.);

- e. Accommodate risk assessments, vulnerability scans, and penetration tests of their server by Clarendon College-IT and take steps to mitigate the risks identified by these procedures.
- f. Immediately report system compromises and other security incidents to the ISO.

10. Internet connectivity is ubiquitous across the campus. Virtually all rooms and meeting spaces at Clarendon College are equipped with wired or wireless connectivity. Nevertheless, facility reservations do not necessarily include the right to use the College network. Consistent with the Acceptable Use Policy, the College cannot guarantee audio or video streaming support by reserving parties.

- a. Departments that accept facility reservation requests from external parties will ascertain the party's need for audio or video transmissions and consult with Clarendon College-IT.
- b. To assure compliance with this provision, departments administering building or room reservations should include the following (or similar) statement on all reservation applications and request forms: "Streaming of audio or video is not permitted from this facility without advance notice and consultation. The reserving party declares that it – DOES / DOES NOT (circle one) – wish to stream audio or video from this facility."

DEFINITIONS:

Application Owner: The individual or group responsible for a specific service or application.

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Dial-Up Server: Refers to connecting a device to a network via a modem and a public telephone network.

Encryption: The conversion of data into a form called cipher text that unauthorized people cannot easily understand.

Hub: A connection point for devices in a network to connect segments of a LAN.

Firewall: A network security system that controls the incoming and outgoing traffic based on applied rule sets.

Information Resources Manager (IRM): Officer responsible for the State of Texas managing Clarendon College's information technology resources. This is the Vice President of Information Technology.

Network Address: A network address (Internet Protocol (IP) address) serves as a unique identifier for a computer on a network.

Network Address Translator: Translating an Internet Protocol (IP) address used within one network to a different IP address known within another network.

Network Scan: The procedure for identifying active hosts on a network for network security assessments.

Penetration Test: Security-oriented probing of a computer system, network, or web application to seek out vulnerabilities that an attacker could exploit.

Personal Firewall: A software application that protects a single internet-connected computer from intruders (sometimes called a desktop firewall).

Proxy Server: A server that sits between a client and an external network to allow clients to make indirect network connections to other network services.

Radiofrequency (RF) spectrum: Any frequency associated with radio wave propagation within the electromagnetic spectrum.

Risk Assessment: A systematic process of identifying, evaluating, and estimating the risks involved in a process or system, their comparison against benchmarks or standards, determining appropriate ways to eliminate or control the hazard, and determining an acceptable level of risk.

Router: A device connected to at least two networks forwards data packets from one network to another.

Server Owner: The individual or group responsible for daily managing a specific application server.

Switch: A managed connection point for devices in a network to connect segments of a LAN.

Virtual Private Network (VPN) Server: A server that extends a private network across a public network, like the internet, to provide remote offices or individuals with secure access to the Clarendon College network using special hardware and software.

Vulnerability: A flaw or weakness in hardware, software, or processes that exposes a system to compromise.

Vulnerability Assessment: The process of identifying, quantifying, and prioritizing a system's vulnerabilities (weaknesses).

Wireless Access Point: A device that allows wireless devices to connect to a wired network using Wi-Fi.

Wired Connectivity: A term to describe any computer connection or network where the connection between sender and receiver involves cables, such as Ethernet.

Wireless Connectivity: A term used to describe any computer connection or network with no physical wired connection between sender and receiver.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
IT Physical Access & Environmental Policy:

PURPOSE:

This policy is intended to establish standards for securing Clarendon College-IT data centers, network closets, and protected IT facilities on the Clarendon College campuses. Effective implementation of this policy will minimize unauthorized access to these locations, provide more effective auditing of physical access controls, and ensure environmental threats to Clarendon College-IT data centers are monitored and remediated promptly.

SCOPE:

The IT Physical Access Policy applies to Clarendon College-IT data centers containing enterprise systems and other information processing facilities such as network closets, on-site backup storage locations, and the corresponding network infrastructure and access across campus that serve the Clarendon College user community.

POLICY STATEMENT:

Clarendon College-IT is responsible for the safety and security of data on the Clarendon College network and the equipment used to run the network infrastructure.

1. Environmental conditions in all data centers will be monitored and protected from environmental threats commensurate with the identified risks and their importance to Clarendon College's mission-critical business processes.
2. Physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
3. Physical access to all restricted information technology resource facilities must be documented and managed.
4. All information technology resource facilities must be physically protected in proportion to the criticality or importance of their function at Clarendon College.
5. Access to information technology resource facilities must be granted only to Clarendon College support personnel and contractors whose job responsibilities require access.
6. The process of granting card and/or key access to information technology resource facilities must include the approval of the person responsible for the facility.
7. Each individual who is granted access rights to an information technology resource facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements
8. Requests for physical access must come from Clarendon College-IT.
9. Access cards and/or keys must not be shared or loaned to others.

10. Access cards and/or no longer required keys must be returned to the appropriate department. Keys or cards must not be reallocated to another individual, bypassing the return process.
11. The appropriate department must report lost or stolen access cards and/or keys immediately.
12. All information technology resource facilities that allow visitor access will track access with a sign-in/out log.
13. Visitors must be escorted in card access controlled areas of information technology resource facilities.
14. A service charge may be assessed for access cards and/or keys lost, stolen, or not returned.
15. Card access records and visitor logs for information technology resource facilities must be kept for routine review based on the criticality of the protected information resources.
16. The person responsible for the information technology resource facility must promptly remove the card and/or key access rights of individuals who change roles within Clarendon College or are separated from their relationship with Clarendon College.
17. The person responsible for the information technology resource facility must periodically review access records and visitor logs and investigate any unusual access.
18. The person responsible for the information technology resource facility must review card and/or key access rights for the facility periodically and remove access for individuals who no longer require access.
19. Restricted access rooms should be identified with discrete signage.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on July 15, 2023.

Appendix A: Authorized Personnel List

The following positions are authorized to access Clarendon College Information Technology (IT) data centers.

Location	Position
Main Campus, ALL	Clarendon College President
	Vice President of Academics Affairs
	IT Support Staff
	Vice President of IT
	Director of Maintenance and Ground
	Director of Custodial Services
Pampa Center, Pampa Only	Dean of the Pampa Center
Childress Center, Childress Only	Dean of the Childress Center

NOTE:

Those identified as having access to "All" locations may grant limited access to any IT data center.

Those identified as having access to a specific location may grant limited access to only that location's IT data center.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Policy Compliance:

PURPOSE

This policy ensures an information technology infrastructure that promotes the college's mission. Clarendon College's information services network has been established for the use and benefit of Clarendon College in the conduct of its academic, business, and other operations. This document provides direction and support for the Clarendon College Information Security Program and the Information Technology (Clarendon College-IT) Policies.

This framework of IT security policies collectively represents the basis of the institutional Information Security program and, on the aggregate whole, meets the objectives articulated by Texas Administrative Code Chapter 202 (TAC§202), Texas Higher Education Coordinating Board (THECB), and the associated guidelines.

This policy promotes the following goals:

1. To ensure the integrity, reliability, availability, and performance of Clarendon College information technology resources;
2. To ensure that the use of Clarendon College information technology resources is consistent with the principles and values that govern Clarendon College as a whole;
3. To ensure that information technology resources are used for their intended purposes; and
4. To ensure all individuals granted access privileges to Clarendon College information technology resources clearly understand what is expected during use and the consequences of violating Clarendon College policies.

SCOPE

This program applies equally to all individuals granted access privileges to Clarendon College information technology resources.

POLICY STATEMENT

Information technology resources are integral to fulfilling the college's primary mission. Users of Clarendon College's information technology resources are responsible for protecting and respecting those resources and knowing the regulations and policies that apply to appropriately using the college's information technology resources.

Users must understand the expectation that, if needed, Clarendon College's information technology resources may be limited and/or regulated by Clarendon College to fulfill the primary mission of the college. Usage may be constrained to assure adequate capacity, optimal performance, and appropriate security of those resources.

Anyone using Clarendon College's information resources expressly consents to monitoring of the network by the college at any time and for any purpose, including but not necessarily limited to evidence of possible criminal activity, violations of law, contract, copyright, or patent infringement, and/or violation of any college policy, rule, or regulation.

Clarendon College's information security policies can be found on the College's website at: <https://www.clarendoncollege.edu/information-technology>.

The Information Security User Guide, which contains a summary of user-related policies, can be found at: [http://\[LINK TO SECURITY GUIDE\]](http://[LINK TO SECURITY GUIDE])

The Information Security Program, which contains the framework, ensures that the appropriate safeguards are applied to Clarendon College's information systems. The program document can be found at: [http://\[LINK TO INFO SECURITY PROGRAM\]](http://[LINK TO INFO SECURITY PROGRAM])

A review of the institution's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or their designated representative(s). TAC 202.76(c)

NON-CONSENSUAL ACCESS

Clarendon College cannot guarantee the privacy or confidentiality of electronic documents. Consequently, persons that use these Clarendon College-owned resources, or any personally owned device that may be connected to a Clarendon College resource, have no right to privacy in their use of these resources and devices. However, Clarendon College will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that Clarendon College will not seek access to their electronic messages or documents without their prior consent except where necessary to:

1. Satisfy the requirements of the Texas Public Information Act or other statutes, laws, or regulations;
2. Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
3. Protect the integrity of Clarendon College's information technology resources and the rights and other property of Clarendon College;
4. Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergencies or
5. Protect the rights of individuals working in collaborative situations where information and files are shared.

To appropriately preserve the privacy of electronic documents and allow authorized individuals to perform their assigned duties, specific college staff and law enforcement will sign a Clarendon College Non-Consensual Access to Electronic Information Resources Request Form annually and submit it to the Vice President of Information Technology. At the beginning of each fiscal year, non-consensual access requests will be resubmitted, reviewed,

and approved or denied by the VPIT.

Individuals may request non-consensual access to specific data by initiating the Non-Consensual Access to Electronic Information Resources Request Form, obtaining the approval of their organizational head, and submitting the form to the Vice President of Information Technology (VPIT). If the request appears compliant with college policy, the DIS or designee will coordinate with the Information Security Officer (ISO) as necessary to satisfy the request.

VIOLATIONS

Failure to adhere to the provisions of the information technology security policies may result in:

1. suspension or loss of access to institutional information technology resources
2. appropriate disciplinary action under existing procedures applicable to students, faculty, and staff and
3. civil or criminal prosecution

Potential violations will be investigated consistent with applicable laws and regulations and Clarendon College policies, standards, guidelines, and practices.

EXCEPTIONS TO POLICY

Exceptions are granted case-by-case and must be reviewed and approved by the College designated VPIT. The required Policy Exception Form and procedures can be found at [http://\[LINK TO POLICY EXEMPTION FORM\]](http://[LINK TO POLICY EXEMPTION FORM]). The IRM will mandate the documentation and additional administrative approvals required to consider each policy exception request.

REFERENCE

Many individual laws, regulations, and policies establish our information security requirements. The primary applicable references are listed below.

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Government Code, Title 5, Subtitle A, Chapter 552
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)

- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 19, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Portable Computing Policy:

PURPOSE:

Clarendon College may, at its discretion, provide portable computing devices and media to employees. The portability offered by these devices and media increases the risk of unauthorized disclosure of stored information.

To maintain the confidentiality, integrity, and availability of data and network resources at Clarendon College, the Portable Computing Policy establishes requirements for safeguarding electronic devices that can contain protected data.

SCOPE:

The Clarendon College Portable Computing Policy applies to all individuals who use portable computing devices and media, whether Clarendon College-issued or privately owned, to access the Clarendon College information technology computing environment.

POLICY STATEMENT:

Clarendon College's policy is to protect mobile computing devices and the information on such devices. Individuals who use these devices must protect the hardware provided from theft and unnecessary damage and the data stored on them.

As a general practice, sensitive information should only be stored on servers. Data owners must carefully evaluate the risk of lost or stolen data against efficiencies related to mobile computing before approving the storage of confidential or sensitive information on portable computing devices.

The users of portable computing devices or media used to store, transmit, or process protected data are expected to take all appropriate measures and precautions to prevent the loss, theft, damage, and/or unauthorized use and shall include the following:

1. Physically and logically safeguard the devices.
2. Ensure that College-approved anti-malicious software applications and signatures are up-to-date.
3. Use encryption to safeguard all storage media (e.g., hard drives, USBs).
4. Avoid unsecured or untrusted networks.
5. Confidential information should not be accessed over unsecured or untrusted networks.
6. Confidential information should not be stored on a portable computing device.
7. Installing mobile device security software on all college mobile computing systems to secure and track all mobile computing devices, i.e., tablets and laptops.
8. Prevent the use of the portable computing device or media by unauthorized persons;

are responsible for any misuse of the information by persons to whom they have given access.

9. All reasonable precautions to prevent data compromise should be taken when using portable computing devices (e.g., shield screen from passive viewing, password-protected screen saver).
10. Keep portable computing devices within view or securely stored.
11. Ensure the device is shut down or secured when not used (e.g., password-protected devices offering such capabilities).
12. Unattended portable computing devices must be physically secure (e.g., locked in an office, desk drawer, or filing cabinet; in an automobile, safe in a non-visible location).
13. Promptly notify Clarendon College-IT if any portable computing device or media has been lost or stolen.

Requests for exceptions to this policy must be submitted in writing and will be reviewed on a case-by-case basis, see Compliance Policy and Policy Exemption Form. To address a specific circumstance or business need, the Vice President of Information Technology may grant an exception to the encryption requirement for portable devices.

DEFINITIONS:

Encryption: At its most basic level, encryption protects information or data using mathematical models so that only the parties with the key to unscramble it can access it.

Malicious Software: A term used to describe any code in any part of a software system or script intended to cause undesired effects, security breaches, or damage to a system.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>.

The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE IT)
Privacy Policy:

PURPOSE:

The Privacy Policy aims to communicate privacy expectations to Clarendon College information technology resource users. It will define standards for managing and enforcing security on any information stored or passing through Clarendon College information technology resources or any personally owned or third-party device that may be connected to a state-owned resource.

Internal users should not expect personal privacy concerning Clarendon College's information technology resources. Information technology resources provided by Clarendon College are owned by the State of Texas and subject to state and Clarendon College oversight. Clarendon College's information technology resources may be monitored to manage performance, perform routine maintenance and operations, protect the integrity of Clarendon College's information technology resources, perform security reviews, and fulfill complaint or investigation requirements.

SCOPE:

The Internal Privacy Statements apply equally to all individuals who use Clarendon College information technology resources or connect personally owned devices to Clarendon College information technology resources.

The Public Privacy Statements apply to members of the general public concerned about the types of information gathered and how that information is used.

POLICY STATEMENT:

CLARENDON COLLEGE Internal Privacy:

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of Clarendon College are the property of Clarendon College. These files are not private and may be accessed by authorized Clarendon College-IT employees and campus administration at any time without the knowledge of the information technology resource user or owner.

To manage systems and enforce security, Clarendon College-IT may log, review, and otherwise utilize any information stored on or passing through its information technology resource systems under the provisions and safeguards provided in the Texas Administrative Code § 202 (TAC § 202), Information Resource Standards. For these same purposes, Clarendon College-IT may also capture user activity, such as visiting websites. Third-party and customer information has been entrusted to Clarendon College for business purposes, and all faculty and staff will

do their best to safeguard the privacy and security of this information. Customer account data is confidential, and access will be limited based on business needs.

CLARENDON COLLEGE Website Public Privacy:

Clarendon College maintains the <http://www.clarendoncollege.edu/> website and other Clarendon College-owned or –hosted domains as a public service. Clarendon College's detailed public privacy statement (Web Privacy and Site Link) regarding individual websites, data collection, public forums, and links to other sites is available on the website (Web Privacy and Site Link).

For site management functions, information is collected for analysis and statistical purposes (please refer to CLARENDON COLLEGE [Web Privacy and Site Link Policy](#)). This information is not reported or used in any manner that would reveal personally identifiable information unless Clarendon College is legally required to do so in connection with law enforcement investigations or other legal proceedings.

For site security purposes and to ensure that the site remains available to all users, Clarendon College uses software to monitor network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage, which is strictly prohibited and may be punishable under applicable state and federal laws.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 19, 2025.

Clarendon College



Prohibited Technologies Security Policy

Date: January 31, 2025

Version: 1.2

TABLE OF CONTENTS

Table of Contents.....	2
1.0 Introduction	3
1.1 Purpose.....	3
1.2 Scope	3
2.0 Policy.....	3
2.1 State-Owned Devices	3
2.2 Personal Devices Used For State Business	4
2.3 Identification of Sensitive Locations	4
2.4 Network Restrictions	5
2.5 Ongoing and Emerging Technology Threats	5
3.0 Policy Compliance	5
4.0 Exceptions	6
5.0 Version History	6
Addendum A	8

1.0 INTRODUCTION

1.1 PURPOSE

On December 7, 2022, Governor Greg Abbott required (https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf) all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan to guide state agencies on managing personal devices used to conduct state business.

In addition to TikTok, **Clarendon College** may add other software and hardware products with security concerns to this policy and will be required to remove prohibited technologies on the DIR prohibited technology list. Throughout this Policy, "Prohibited Technologies" shall refer to TikTok and any additional hardware or software products added to this Policy.

1.2 SCOPE

This policy applies to all **Clarendon College** full and part-time employees, including contractors, paid or unpaid interns, and users of state networks. All **Clarendon College** employees are responsible for complying with the terms and conditions of this policy.

2.0 POLICY

2.1 STATE-OWNED DEVICES

Except where approved exceptions apply, the use or download of prohibited applications or websites is not permitted on all state-owned devices, including cell phones, tablets, desktop and laptop computers, and other internet-capable devices.

The **Clarendon College** must identify, track, and control state-owned devices to prohibit the installation of or access to all banned applications. This includes the various prohibited applications for mobile, desktop, or other internet-capable devices.

The **Clarendon College** must manage all state-issued mobile devices by implementing the security controls listed below:

- a. Restrict access to "app stores" or non-authorized software repositories to prevent unauthorized applications from being installed.
- b. Maintain the ability to wipe non-compliant or compromised mobile devices remotely.
- c. Maintain the ability to uninstall unauthorized software from mobile devices remotely.
- d. Deploy secure baseline configurations for mobile devices, as determined by **Clarendon College**.

2.2 PERSONAL DEVICES USED FOR STATE BUSINESS

Employees and contractors may not install or operate prohibited applications or technologies on any personal device used to conduct state business. State business includes accessing state-owned data, applications, email accounts, non-public-facing communications, state email, VoIP, SMS, video conferencing, CAPPs, Texas.gov, and other state databases or applications.

Suppose an employee or contractor has a justifiable need to allow personal devices to conduct state business. In that case, they may request that their device be enrolled in the agency's "Bring Your Device" (BYOD) program.

2.3 IDENTIFICATION OF SENSITIVE LOCATIONS

Sensitive locations must be identified, cataloged, and labeled by the agency. A sensitive location is any location, physical or logical (such as video conferencing or electronic meeting rooms), that is used to discuss confidential or sensitive information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

Unauthorized devices such as personal cell phones, tablets, or laptops may not enter sensitive locations, which includes any electronic meeting labeled as a sensitive location.

Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations.

2.4 NETWORK RESTRICTIONS

DIR has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, **Clarendon College** will also implement additional network-based restrictions to include:

- a. Configure agency firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
- b. Prohibit personal devices with prohibited technologies from being installed and connected to agency or state technology infrastructure or data.
- c. Provide a separate network for access to prohibited technologies with the approval of the executive head of the agency.

2.5 ONGOING AND EMERGING TECHNOLOGY THREATS

To protect against ongoing and emerging technological threats to the state's sensitive information and critical infrastructure, DPS and DIR will regularly monitor and evaluate additional technologies posing concerns for inclusion in this policy.

DIR will host a site that lists all prohibited technologies, including apps, software, hardware, and technology providers. The prohibited technologies list current as of January 23, 2023, can be found in Addendum A. New technologies will be added to the list after consultation between DIR and DPS.

Clarendon College will implement the removal and prohibition of any listed technology. **Clarendon College** may prohibit technology threats in addition to those identified by DIR and DPS.

3.0 POLICY COMPLIANCE

All employees shall sign a document annually confirming their understanding of this policy.

Compliance with this policy will be verified through various methods, including but not limited to IT/security system reports and feedback to agency leadership.

An employee found to have violated this policy may be subject to disciplinary action, including termination of employment.

4.0 EXCEPTIONS

Exceptions to the ban on prohibited technologies may only be approved by the executive head of **Clarendon College**. This authority may not be delegated. All approved exceptions to the TikTok prohibition or other statewide prohibited technology must be reported to DIR.

Exceptions to the policy will only be considered when the use of prohibited technologies is required for a specific business need, such as enabling criminal or civil investigations or sharing information with the public during an emergency. For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period. To the extent practicable, exception-based use should only be performed on devices not used for other state business and non-state networks. Cameras and microphones should be turned off on devices for exception-based use.

5.0 VERSION HISTORY

This table summarizes the significant edits, i.e., edits affecting transition points, process changes, system changes, and/or role changes.

Version	Date	Responsible	Revision Summary
1.0	January 26, 2023	Name	Document Creation

6.0 RELATED POLICIES, REFERENCES, AND ATTACHMENTS:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on July 17, 2023, version 1.1. This policy was reviewed by Will Thompson, Vice President of IT, on July 15, 2023.

ADDENDUM A

The up-to-date list of prohibited technologies is published at <https://dir.texas.gov/information-security/prohibited-technologies>. The following list is current as of January 23, 2023.

Prohibited Software/Applications/Developers

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet
- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office
- RedNote
- DeepSeek
- Webull
- Tiger Brokers
- Moomoo
- Lemon8
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware/Equipment/Manufacturers

- Huawei Technologies Company
- ZTE Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company
- SZ DJI Technology Company
- Hytera Communications Corporation

- Any subsidiary or affiliate of an entity listed above.

The Clarendon College Board of Regents approved this policy on _____, version

1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Remote Desktop/Virtual Private Network Access Policy:

PURPOSE:

The Remote Desktop/Virtual Private Network Access Policy exists to protect Clarendon College's information technology resources. Restricting remote access partly ensures the security of the information technology resources in the Clarendon College domain. Remote Desktop (RDP) or Virtual Private Network (VPN) allows Clarendon College users (Regular and Visitor Account users as defined in Policy) to securely access the university's network via an existing connection to the Internet from a remote location.

RDP or VPN connections present an increased security risk if the connecting computer is insecure. Security, Internet access, and configuration of the connecting computer are solely the responsibilities of the user account holder making the connection.

SCOPE:

The Clarendon College Remote Desktop/Virtual Private Network Access policy applies equally to all individuals with authorized RDP or VPN accounts accessing Clarendon College information technology resources.

POLICY STATEMENT:

1. individuals with RDP and/or VPN privileges are responsible for ensuring that unauthorized users are not allowed access to the Clarendon College network using their security credentials.
2. RDP/VPN authentication is controlled using Clarendon College user account credentials.
3. Clarendon College-IT manages RDP/VPN gateways.
4. All computers connected to the Clarendon College network via RDP/VPN or any other technology must use the most up-to-date anti-virus software, regardless of the type or ownership of the device.
5. RDP/VPN users will be automatically disconnected from Clarendon College's network after a designated time-out period determined by Clarendon College-IT. The user must then log in again to reconnect to the network.
6. Pings or other network utilities must not be used to keep the RDP/VPN connection open.
7. Non-Clarendon College-owned equipment must be configured in compliance with Clarendon College policies and procedures.
8. Using RDP/VPN technology with personal equipment, users must understand that their machines are a de facto extension of Clarendon College's network. RDP/VPN users and privately owned equipment must comply with Clarendon College policies and procedures.

9. RDP/VPN access does not guarantee all campus systems/applications access. Access to systems/applications will be evaluated on a case-by-case basis.

DEFINITIONS:

Unauthorized user: A person without official permission or approval to access Clarendon College systems.

Virtual Private Network (VPN): Extends a private network across a public network, like the internet, to provide remote offices or individuals with secure access to the Clarendon College network using special hardware and software.

Remote Desktop (RDP): A program or an operating system feature that allows a user to connect to a computer in another location, see that computer's desktop, and interact with it as if it were local

A VPN Gateway (Also known as a VPN Router) is a connection point connecting two networks connected by a non-secure network such as the Internet.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
System Information Technology Services (CLARENDON COLLEGE-IT)
IT Risk Assessment Policy:

PURPOSE:

IT risk assessments are designed to assess the security posture of a system or application to ensure management's awareness of the significant security risks in the Clarendon College infrastructure and recommend mitigation plans for these risks.

The principal goal of a risk management process is to protect the College and its ability to perform its mission. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system but as an essential management function of the College.

Risk assessments will be conducted annually, as directed by the state, and/or on an ad-hoc basis in response to specific events, such as when significant modifications are made to the system's environment or in response to a security incident or audit.

SCOPE:

The Clarendon College Risk Assessment Policy applies to all stakeholders involved in preserving the confidentiality, integrity, and availability of information technology resources. Stakeholders include but are not limited to, Clarendon College administration, application administrators, system administrators, data owners, users, and information security personnel.

POLICY STATEMENT:

Appropriate security levels and data control requirements must be determined for all information technology resources based on Clarendon College confidentiality, integrity, and availability requirements for the information, as well as its criticality to Clarendon College's mission and legal requirements.

Information technology risk analysis and management processes require gathering a broad range of data on information technology assets and potential threats. The data collection phases of the risk management process include an information technology asset inventory consisting of server build documentation, network penetration tests, logs, patch histories, and other vulnerability assessment tools for essential assets.

The ISO shall periodically (at least annually) complete or commission a risk assessment of the information resources considered essential to the College's critical mission and functions. It shall recommend appropriate risk mitigation measures, technical controls, and procedural safeguards to the owners and custodians of these resources.

The assessment may incorporate self-assessment questionnaires, vulnerability scans, scans for confidential information, and penetration testing. Findings and recommendations shall be provided to the owners and custodians of the information assets. They shall also be presented

to the Vice President of Information Technology and members of the IT Governance Committee for sharing with the president as appropriate.

The key roles of personnel who are responsible for the protection of Clarendon College information technology resources and participate in the risk management/assessment process can be found in the Clarendon College Information Security Program at [http://\[LINK TO INFORMATION SECURITY PROGRAM\]](http://[LINK TO INFORMATION SECURITY PROGRAM]). Roles include Data Owner or designated representative(s), Data Custodian(s), Users, Information Security Officer (ISO), and Information Resources Manager.

DEFINITION:

Network Penetration Test: A pen test is an authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data.

IT Governance Committee: A group that oversees an organization's IT strategy, systems, financing, and risk management. The committee's role is to ensure the organization's IT investments align with its goals. A committee consisting of the President, Vice President of Academic Affairs, and the Vice President of Information Technology.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Security Breach Notification Policy:

PURPOSE:

This policy is intended to ensure that all Clarendon College personnel know the college's responsibilities under the law.

This policy governs the actions of any Clarendon College official (defined below) who discovers or is notified of a breach or possible breach of the security of unencrypted personal information collected and retained by Clarendon College as computerized data.

This document establishes specific requirements for using all computing and network resources at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C ([TAC§202](#)) and Texas Higher Education Coordinating Board)

This policy and the Clarendon College Technology Incident Management Policy should be used.

SCOPE:

This breach can result from a compromise of a Clarendon College computing system or network, the loss or theft of any physical device in which personal information is stored, or any storage medium upon which personal information is maintained.

Clarendon College maintains computerized data on various college systems, including personal information. Suppose the security of any Clarendon College system storing or processing automated data that includes unencrypted personal information is compromised. In that case, the owner or licensee of that information must be notified by the college of the system's breach if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

RIGHTS AND RESPONSIBILITIES:

Good faith acquisition of personal information by a Clarendon College official with a legitimate educational interest in the data or information is not a breach of the system's security when the personal information is not used or subject to further unauthorized disclosure. Clarendon College is not required to disclose a technical violation of system security, which does not seem reasonably likely to subject the owners of personal information stored on those systems to risk criminal activity.

All college officials must comply with and understand the responsibilities expressed in this policy. Certain Clarendon College administrative personnel also have additional responsibility for the maintenance and execution of this policy.

POLICY STATEMENT:

1. This disclosure shall be made as expediently as possible following discovery or notification of the breach—without unreasonable delay and consistent with any measures taken to determine the scope of the breach and restore the integrity of the affected data system. This notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In that case, the notification may be made after the law enforcement agency determines that such notification does not compromise an ongoing investigation.
2. Any college official who discovers or is notified of a breach of the security of any Clarendon College technology system will report it. The initial report of a potential security breach involving computerized data will likely be made in one of three ways:
 - a. A report to the Clarendon College Vice President of Information Technology of the theft of a computing or storage device.
 - b. If the presenting incident is a theft, the Vice President of Information Technology will:
 - i. Report it to law enforcement and act as liaison with any law enforcement agency involved in the situation;
 - ii. Notify the Comptroller of the incident,
 - iii. Notify the Vice President of Academic Affairs (or designee), and
 - iv. Notify the Vice President of Student Affairs (or designee) of the incident.
 - v. Follow routine computing services inventory procedures regarding loss or theft of technology;
3. The discovery of a breach of security of a computer or the Clarendon College network by support staff.
 - a. If the presenting incident is the discovery of a network breach, the Vice President of Information Technology will:
 - i. Begin network and computer technical investigations following the guidelines articulated in the Clarendon College IT security standard addressing intrusion detection and incident response. This will continue until the security and technical aspects of the situation are resolved.
 - ii. Notify the Comptroller of the incident,
 - iii. Notify the Vice President of Academic Affairs (or designee), and
 - iv. Notify the Vice President of Student Affairs (or designee) of the incident.
4. In some circumstances, it may be appropriate to report a breach of the network's security or Clarendon College computers to law enforcement.
 - a. The Vice President of Information Technology (or designee) and the Comptroller (or designee) will consult regarding the nature and scope of the security breach and determine whether law enforcement needs to be notified.
 - b. The Vice President of Information Technology (or designee) will notify the Vice President of Academic Affairs and the Vice President of Student Affairs (or designees) regarding the incident and will have responsibility for guiding the initial investigation by IT technical representatives into the situation and determining the nature of any unencrypted data which may have been compromised.
5. If it is determined that a breach may have compromised the security, confidentiality, or integrity of Clarendon College-managed personal information, the Vice President of

Academic Affairs (or designee) will initiate a meeting as soon as possible of the college's Incident Response Team, consisting of the following or their designees:

- a. Vice President of Academic Affairs (chair).
 - b. Vice President of Student Affairs.
 - c. Comptroller.
 - d. Registrar (if student data may be involved) and/or Payroll/Benefits Coordinator (if staff data may be involved).
 - e. Vice President of Information Technology.
6. The Vice President of Information Technology will notify the college president that the Incident Response Team has been activated and will provide updates regarding actions taken, as appropriate.
7. The Incident Response Team will:
- a. Assign from the team membership a scribe responsible for maintaining notes, minutes, and a final written report to the college president regarding the incident, its resolution, and the institutional response.
 - b. Gather information regarding the situation and the type and nature of the unencrypted data that has potentially been compromised.
 - c. Determine if a legal responsibility exists to notify individuals that their personal information has or may have been disclosed.
 - d. Determine who is affected by the breach and should be notified.
 - e. Determine which of the methods of disclosure (below) prescribed by law is appropriate.
 - f. Assign appropriate tasks to team members based on their institutional responsibilities and expertise. The team will determine these tasks based on the specific situation.
 - g. Conduct a debriefing meeting to review and approve the report to the college president once the situation is resolved.
8. Notification of disclosure of personal information may be made in one of the following methods:
- a. Written notice.
 - b. Electronic notice consistent with the provisions regarding electronic records and signatures outlined in 15 U.S.C. Sec. 7001.
 - c. Substitute notice. This is allowed if the cost of providing notice to all affected individuals exceeds a reasonable amount or Clarendon College does not have sufficient contact information. Substitute notice is defined as ALL of the following:
 - i. E-mail notice when Clarendon College has an e-mail address for the subject persons,
 - ii. Conspicuous posting of a notice on Clarendon College's website and
 - iii. Notification to major statewide media.

DEFINITIONS:

College Official: Clarendon College defines a college official as:

1. A person the college employs in an administrative, supervisory, academic research, or support staff position.
2. A person appointed to the board of regents.

3. A person assigned, employed by, or under contract to the college to perform a special task, such as an attorney or auditor.
4. A person who is employed by public safety.
5. A student serving on an official committee, such as a disciplinary or grievance committee, or assisting another college official in performing their tasks.

Legitimate Educational Interest: Clarendon College defines a college official who has a legitimate educational interest as one who is:

1. Performing a task specified in their position description or contract agreement.
2. Performing a task related to a student's education.
3. Performing a task related to the discipline of a student.
4. Providing a service or benefit relating to the student or student's family, such as health education, Counseling, advising, student employment, financial aid, or other student service-related assistance.
5. Maintaining the safety and security of the campus.
6. Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at

<https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE IT)
Security Contracts and Cloud Services Procurement Policy

Clarendon College is committed to maintaining a secure IT environment that aligns with TX-RAMP, StateRAMP, and FedRAMP requirements and industry best practices. This policy outlines the guidelines for IT security management and contractual agreements that integrate TX-RAMP and StateRAMP standards.

PURPOSE:

The purpose of this policy is to establish comprehensive IT security management practices and contractual requirements that align with TX-RAMP and/or StateRAMP guidelines as described here: <https://prod.dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp>. This policy aims to protect the college's digital assets, ensure compliance with Texas regulations, and foster a culture of cybersecurity awareness.

SCOPE:

This policy applies to all college departments, personnel, contractors, vendors, and external parties engaged in IT security management and contractual relationships related to IT services, systems, or data within Clarendon College in Texas.

POLICY:

1. IT Security Management

- a. Risk Assessment: Regular risk assessments will be conducted to identify vulnerabilities and threats. The assessments will consider TX-RAMP and/or StateRAMP requirements and Texas-specific security considerations.
- b. Security Controls: TX-RAMP and/or StateRAMP security controls will serve as the baseline for implementing measures to mitigate risks and meet compliance standards specific to Texas (Texas Government Code [2054.003 \(13\)](#)).
- c. Access Management: External user access privileges will be granted based on the principle of least privilege, aligning with TX-RAMP and/or StateRAMP principles and state regulations.
- d. Security Training: Ongoing security training will be provided to personnel, integrating TX-RAMP and StateRAMP guidelines and state-specific cybersecurity regulations.

2. IT Contracts

- a. Security Requirements: All IT contracts must adhere to TX-RAMP or StateRAMP security measures and controls requirements. Contracts will also account for Texas-specific legal and regulatory obligations.

- b. Data Protection: Contracts must address protecting personal and sensitive data by TX-RAMP and/or StateRAMP and Texas data protection standards.
- c. Compliance: Vendors must demonstrate compliance with either TX-RAMP, StateRAMP, FedRAMP, or Texas regulations, including relevant cybersecurity and data protection laws.
- d. Incident Response: Contracts should outline vendors' responsibilities during a security incident, considering TX-RAMP and StateRAMP incident response procedures and state-specific reporting requirements.

3. Reporting and Compliance

- a. Incident Reporting: All security incidents or breaches, aligning with TX-RAMP or StateRAMP and Texas regulations, must be promptly reported to the college's IT security team for investigation and response.
- b. Contract Compliance: College departments and personnel overseeing IT contracts ensure that vendors meet TX-RAMP, StateRAMP, or FedRAMP and Texas-specific security requirements. A listing of TX-RAMP-certified Cloud products can be found here: <https://prod.dir.texas.gov/resource-library-item/tx-ramp-certified-cloud-products>.

4. Consequences of Non-Compliance

- a. Non-compliance with either TX-RAMP, StateRAMP, or FedRAMP and Texas IT security practices or contractual obligations may result in disciplinary actions, contract termination, or other appropriate measures.

DEFINITIONS:

TX-RAMP: The Texas Risk and Authorization Management Program (TX-RAMP) provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process, store, or transmit the data of a state agency. More information can be found here: <https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp>.

StateRAMP: StateRAMP is a non-profit governed by most state and local government officials, who adopt policies that guide the security verification requirements and process. Committees help inform the policies and provide opportunities for participation from those in both the public and private sectors. More information can be found here: <https://stateramp.org/>,

FedRAMP: The Federal Risk and Authorization Management Program (FedRAMP®) was established in 2011 to provide a cost-effective, risk-based approach to the federal government's cloud services adoption and use. More information can be found here: <https://www.fedramp.gov/>.

Cloud Computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model comprises five essential characteristics, three service, and four deployment models. See NIST SP 800-145, The NIST Definition of Cloud Computing | CSRC.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Server Administration Policy:

PURPOSE:

This policy establishes the framework to protect Clarendon College servers against unauthorized access, disclosure, modification, or destruction and to assure information availability, integrity, authenticity, and confidentiality. A server is a computer system dedicated to providing services, as a host, to serve the needs of the users of other computers on the network.

This policy establishes standards for the base configuration of server equipment (physical or virtual devices), licensing, unnecessary services, default passwords, and disconnection/isolation of threatening servers owned and/or operated by Clarendon College.

SCOPE:

The Clarendon College Server Administration policy applies to any servers owned or managed by Clarendon College.

POLICY STATEMENT:

All Clarendon College-owned or managed servers will comply with the requirements outlined in this and related Clarendon College policies, TAC§202 (Subchapter C), and other state and federal guidelines and requirements.

1. Server configuration standards and procedures are established and maintained by the Vice President of Information Technology or any company acting on behalf of the Clarendon College IT and approved by the Information Security Officer (ISO).
2. The Information Resources Manager (IRM) is ultimately responsible for managing Clarendon College's information technology resources.
3. All servers must be physically secure and safeguarded in compliance with the IT Physical Access & Environmental Policy. Servers are expressly prohibited from operating from uncontrolled cubicles and office areas.
4. Access control logs will be posted outside all server or network control rooms.
5. All servers that connect to the Clarendon College network must be installed, configured, and managed by the Clarendon College IT.
6. The Clarendon College-IT must:
 - a. Install and configure servers according to the Vice President of Information Technology's standard build documents and procedures, to include (but not limited to):
 - i. Install an appropriately licensed server operating system and antivirus protection software.
 - ii. Make every effort to adhere to the latest applicable security configuration benchmarks published by the Center for Internet Security (CIS).

- iii. Disable all default accounts except those required to provide necessary services.
 - iv. Install the most recent security patches as soon as practical, according to the Change Management Policy.
 - v. Disable all services and applications not required for the server to meet its mission (e.g., Telnet, FTP, DNS, DHCP, and SMTP on a file server).
 - vi. Include standard security principles of least-required access to perform a function (e.g., do not use root access when a non-privileged account will do).
- b. Install appropriately licensed software required by the Data Owner or Application Administrator.
 - i. Disable all application default accounts except those required to provide necessary services.
 - ii. Change the application default passwords for all enabled accounts to one consistent with the Clarendon College User Accounts Password Policy.
- c. If a methodology for secure channel connection is necessary, privileged access must be performed over secure channels (e.g., encrypted network connections using SSH or IPSec).
- d. Servers must perform the necessary vulnerability scans before providing service to the campus or the internet. Any serious vulnerability must be corrected before being placed into production.
- e. Those servers that house confidential College data or provide access to it may be required to meet additional requirements defined by the appropriate data owner.
- f. Clarendon College maintains a Clarendon College device registry to facilitate compliance with security policies and procedures and assist in diagnosing, locating, and mitigating security incidents on the College network.
 - i. Servers attached to the Clarendon College network must be registered by Clarendon College-IT and approved by the ISO.
 - ii. Registration must include contact(s) and location, hardware and operating system/version, primary function(s) of the server, associated applications, and demonstrated compliance with the required Clarendon College policies, TAC§202 (Subchapter C) and other state and federal requirements.
 - iii. The ISO will require updating registry information with the annual information security risk assessment process.
- 7. Application Administrators must:
 - g. Enforce the application's usage policies, implement the application-specified access controls, and configure and maintain the server's application according to the required standards.
 - h. Include standard security principles of least-required access to perform a function (e.g., do not grant an administrative account access to the application when a non-privileged account will do).
- 8. Backups should be completed regularly based on a risk assessment of the data and services provided and must comply with the Data Backup Policy.
- 9. Clarendon College-IT will disconnect a server posing an immediate threat to the Clarendon College network to isolate the intrusion or problem and minimize risks.

- i. This can be done without contacting the owner or application administrator if circumstances warrant.
 - j. The server will remain disconnected until it is brought back into compliance or is no longer a threat.
10. Clarendon College cooperates fully with federal, state, and local law enforcement authorities in criminal investigations and will file criminal complaints against users who access or utilize the network to conduct a criminal act.
- k. Under the Clarendon College Technology Incident Management Policy, incident response best practices must be followed to ensure appropriate preservation and treatment of forensic data.
 - l. All logs and audit trails about security-related events on critical or sensitive systems will be managed according to the Clarendon College Technology Incident Management Policy.
 - m. The ISO will:
 - i. Perform periodic reviews to ensure compliance with this policy.
 - ii. Notify the Information Resources Manager (IRM) of identified concerns and risks.
11. Exceptions to the Server Administration Policy must be submitted in writing and approved by the ISO. Requests shall be justified, documented, and communicated during the risk assessment.

DEFINITIONS:

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
System Development & Acquisition Policy:

PURPOSE:

The System Development & Acquisition Policy aims to ensure that security is integral to Clarendon College system planning and management and the business processes associated with those systems.

The procedures for new and changed information systems that contain protected data must integrate information security requirements into the software lifecycle. The security requirements must identify controls to ensure confidentiality, integrity, and availability. These controls must be appropriate and cost-effective and mitigate risks resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the protected data. This is true regardless of whether the systems are purchased, used from community or open-source collaborations, or developed by Clarendon College.

SCOPE:

The System Development & Acquisition Policy applies to all software/systems installed and utilized on Clarendon College information technology resources that contain confidential and/or protected data.

This policy does not apply to faculty or students developing and experimenting with software programs as part of an approved curriculum.

POLICY STATEMENT:

All in-house software that runs in a production environment shall be developed according to the Clarendon College-IT Project Lifecycle Policy and must adhere to the Clarendon College Application Security Policy. At a minimum, this plan shall address the areas of stakeholder identification and involvement, preliminary analysis or feasibility study, risk identification and mitigation, systems analysis, general design, detail design, development, quality assurance and acceptance testing, implementation, and post-implementation maintenance and review. The requirement for such methodology ensures that the software will be adequately documented and tested before it is used for critical information. Additionally, this methodology ensures that projects match the College's strategic direction and comply with guidelines.

Where resources permit, there shall be a separation between the production, development, and test environments. This ensures that security is rigorously maintained for the production system while the development and test environments can maximize productivity with fewer security restrictions. Testing should not be performed using production systems due to the threat to its confidentiality and/or integrity.

All applicable systems shall have designated owners and custodians. Clarendon College-IT shall perform periodic risk assessments of production systems to determine whether the controls employed are adequate.

If an enterprise information system or component of that system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow Clarendon College to test the system's security controls if needed. All acquired software that runs on production systems shall be subject to the Clarendon College-IT Project Lifecycle and must adhere to the Clarendon College Application Security Policy.

An assessment of the system's security controls and a vulnerability assessment must be performed on all new information systems or systems undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production information systems, and appropriate measures must be taken to address the risk associated with identified vulnerabilities.

Clarendon College-IT Change Management Policy will be followed to review and approve a change before it is moved into production.

Opportunities for misuse of information should be appropriately minimized or prevented with risk assessments, monitoring and logs, and end-user awareness and training on preventive strategies.

DEFINITIONS:

Change Management: The controlled identification and implementation of required changes within a business's information technology systems.

Data Custodian: The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Project Lifecycle: A series of activities to fulfill project goals or objectives.

Risk Assessment: A systematic process of identifying, evaluating, and estimating the risks involved in a process or system, their comparison against benchmarks or standards, determining appropriate ways to eliminate or control the hazard, and determining an acceptable level of risk.

System Development & Acquisition: An organization's ability to identify, acquire, install, and maintain appropriate information technology systems. This includes internally developing software applications or systems and purchasing hardware, software, or services from third parties.

Stakeholder: A person or group interested in something, is impacted by it and cares about how it turns out.

Vulnerability Assessment: Identifying, quantifying, and prioritizing a system's vulnerabilities (weaknesses).

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Technology Security Training Policy:

PURPOSE:

Understanding the importance of computer security and individual responsibilities and accountability are paramount to achieving organizational security goals. This will be accomplished with general computer security awareness training and targeted product-specific training. The philosophy of protection and specific security instructions must be taught to and reinforced by technology users. The security awareness and training information needs to be continuously upgraded and strengthened.

The purpose of the Technology Security Training Policy is to describe the requirements that ensure each user of Clarendon College information technology resources receives adequate training on technology security issues. Additionally, state law requires that higher education institutions provide an ongoing information security awareness education program for all users of state-owned information resources (Texas Administrative Code (TAC) §202).

SCOPE:

The Clarendon College Technology Security Training policy applies equally to all employees.

POLICY STATEMENT:

1. All employees must attend the Clarendon College Security Awareness Training within 30 days of initially being granted access to Clarendon College information technology resources or per the request of the data owner or supervisor.
2. Annually, all employees must complete the Clarendon College Security Awareness training and pass the associated examination(s).
3. Annually, all employees must sign a non-disclosure agreement per the Non-Disclosure Agreement Policy stating they have read and understand Clarendon College requirements regarding Clarendon College-IT policies and procedures.
4. Clarendon College-IT must prepare, maintain, and distribute an Information Security User Guide that concisely describes Clarendon College's information security policies and procedures.
5. Clarendon College-IT must develop and maintain a communication plan that will communicate security awareness to the Clarendon College user community.

DEFINITIONS:

Information Security User Guide: Describes the requirements that ensure each person has the knowledge to protect Clarendon College's information technology resources, defend themselves, and comply with applicable laws.

Non-Disclosure Agreement: All employees must sign acknowledging they have read and understand Clarendon College's computer security policies and procedures requirements. This agreement becomes a permanent record and will be renewed annually.

Security Awareness Training: Annual training required by the Texas Administrative Code §202 to re-familiarize users with the Clarendon College policies, their responsibility to protect Clarendon College resources, and to behave responsibly, ethically, and legally.

Texas Administrative Code (TAC) §202): A state law that outlines mandatory user security practices, specifically security awareness training and non-disclosure agreements.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
System Information Technology Services (CLARENDON COLLEGE-IT)
Technology Acquisition Oversight Statement:

PURPOSE:

Clarendon College mandates review and oversight of all information technology resource-related acquisitions. This includes, but is not limited to, computing and networking hardware, software, peripherals, classroom technology, video development, 2-way radios, phones, TVs, security equipment, copiers, fax machines, and various cloud or online services (including electronic subscriptions), regardless of the source of funds and method or location of use. Clarendon College designates the College designated Vice President of Information Technology and their designee to oversee these acquisitions and/or gifts.

SCOPE:

All information technology resource-related acquisitions and gifts must be reviewed by the Clarendon College Information Technology Services Department, and approval must be received before formally submitting a request for acquisition or acceptance of the gift.

POLICY:

Clarendon College-IT and the IT Governance Committee will jointly review acquisitions as necessary to ensure compatibility with existing technology, sustainability, and consistency with campus direction and mission.

DEFINITION:

IT Governance Committee: A group that oversees an organization's IT strategy, systems, financing, and risk management. The committee's role is to ensure the organization's IT investments align with its goals. A committee consisting of the President, Vice President of Academic Affairs, and the Vice President of Information Technology.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Technology Incident Management Policy:

PURPOSE:

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

This document describes the requirements for dealing with computer security incidents. Security incidents include but are not limited to, viruses, worms, ransomware, spyware, Trojan Horse detection, unauthorized use of computer accounts and computer systems, and complaints of improper use of information technology resources as outlined in the Clarendon College policies.

The policy and Clarendon College Security Breach Notification Policy should be used.

SCOPE:

The Clarendon College Technology Incident Management Policy applies to the ISO, IRM, and Incident Response Team (IRT).

POLICY STATEMENT:

1. As an incident is identified, pre-defined roles and responsibilities of the Clarendon College IRT members take priority over regular duties. See Appendix A, Incident Categorization and Prioritization, regarding incident priorities.
2. The ISO is responsible for initiating, completing, and documenting the incident investigation with assistance from the IRT.
3. The ISO is responsible for notifying the IRM, any company acting on behalf of the Clarendon College IT, and the IRT and initiating the appropriate incident management action, including restoration, as defined in the Technology Incident Management Policy.
4. The appropriate Incident Management procedures must be followed whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc., is suspected or confirmed. Also, see the Clarendon College Security Breach Notification Policy.
5. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the Incident Investigation.
6. The appropriate technical resources from the IRT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
7. The ISO, working with the IRM and any company acting on behalf of the Clarendon College IT, will determine if a widespread Clarendon College communication is

- required, the content of the communication, and how best to distribute the communication. The appropriate technical resources from the IRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
8. Clarendon College IT or any company acting on behalf of Clarendon College IT will disconnect a server posing an immediate threat to the Clarendon College network to isolate the intrusion or problem and minimize risks.
 - a. This can be done without contacting the owner or application administrator if circumstances warrant.
 - b. The server will remain disconnected until it is returned to compliance or is no longer a threat.
 9. The Clarendon College ISO is responsible for reporting the incident to the following:
 - a. IRM
 - b. Office of Information Technology Services as outlined in TAC§202
 - c. Local, state, or federal law officials as required by applicable statutes and/or regulations
 10. The ISO coordinates communications with the College media liaison.
 11. If law enforcement is not involved, the ISO will recommend disciplinary actions, if appropriate, to the College President.
 12. In case law enforcement is involved, the ISO will act as the liaison between law enforcement, including the College Security and Clarendon College-IT.
 13. Documentation and reporting are an essential part of incident management. Thorough documentation and reporting must be maintained throughout the incident management process. Detailed records of incident investigations, actions taken, and outcomes achieved are essential. This information will identify trends, measure performance, and support decision-making processes.

DEFINITIONS:

Breach of the Security of the System: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by Clarendon College.

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Incident Response Team (IRT): See Security Breach Notification Policy.

Information Security Officer (ISO): Clarendon College designee with the explicit authority and the duty to administer the information security requirements of Texas Administrative Code TAC 202.71.

Information Resources Management (IRM): The process of managing information resources to accomplish the college's missions and improve its performance, including

reducing information collection burdens on the public. When standardized and controlled, these resources can be shared and reused throughout the college, not just by a single user or application.

Personal Identifiable Information (PII): Defined by statute as an individual's first name or first initial and last name in combination with any one or more of the following data elements:

1. Social Security number;
2. Driver's license number or government-issued ID number, or;
3. Health care information, such as information about an individual's physical or mental health or;
4. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
5. Personal information does not include publicly available information lawfully made available to the general public from federal, state, or local government records.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Appendix A

The following is a listing of incident categorization and prioritization ranked in order of criticality.

1. **Critical Incidents:** These incidents pose an immediate and severe threat to the organization's operations, data, or reputation. Examples include significant data breaches, widespread malware outbreaks, or denial-of-service attacks that impact critical systems or services.
2. **High-Priority Incidents:** These incidents can cause significant disruption or damage if not addressed promptly. Examples include targeted phishing attacks against key personnel, ransomware infections affecting essential systems, or unauthorized access to sensitive data.
3. **Medium-Priority Incidents:** These are incidents that require attention but may not have an immediate impact on critical operations. Examples include isolated malware infections on non-essential systems, minor data leaks involving non-sensitive information, or policy violations by individual users.
4. **Low-Priority Incidents:** These incidents have minimal impact on operations or can be addressed without significant resources or urgency. Examples include routine software glitches, minor network interruptions, or low-risk security alerts that do not require immediate action.
5. **Incident Categories Based on Impact:** Incidents can also be categorized based on their potential impact on confidentiality, integrity, and availability of information assets. For example, incidents affecting sensitive data (such as personal information or financial records) may be prioritized over incidents involving non-sensitive information.
6. **Incident Categories Based on Attack Vectors:** Incidents can be categorized based on the method of attack or exploitation used by threat actors. For example, phishing attacks, malware infections, insider threats, or physical security breaches may each have their category for prioritization and response.
7. **Regulatory Compliance Requirements:** Some incidents may need to be prioritized based on regulatory compliance requirements or legal obligations. For example, incidents involving compromising Personally Identifiable Information (PII) may need to be prioritized to ensure compliance with data protection laws and regulations.
8. **Business Impact Assessment:** Conducting a business impact assessment can help prioritize incidents based on their potential impact on critical business processes, revenue generation, customer trust, or regulatory compliance. Incidents with the

most significant impact on the organization's ability to achieve its objectives may be prioritized higher for response and resolution.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Third Party Access Policy:

PURPOSE:

Clarendon College receives requests for direct connections to its information technology resources from contractors, vendors, and other third parties for support services, contract work, or other remote access solutions.

This policy defines standards for connecting to Clarendon College information technology resources. These standards are designed to minimize the potential exposure to Clarendon College from damages that may result from the unauthorized use of Clarendon College's information technology resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical Clarendon College internal systems, etc.

SCOPE:

The Third-Party Access Policy pertains to all third-party organizations and individuals that require access to non-public electronic resources maintained by Clarendon College.

POLICY STATEMENT:

As a condition of gaining access to Clarendon College information technology resources:

1. Every third party must sign a Clarendon College Non-Disclosure Agreement.
2. A Clarendon College department, organization, or employee must sponsor all third parties.
3. All third-party access must be uniquely identifiable, and password management must comply with the User Accounts Password Policy and Administrator/Special Access Policy guidelines.
4. All third-party account holders must provide contact information that will be used to contact them in the event of account status changes, misuse, or termination of the agreement.
5. All changes to access granted under this policy must originate from the Clarendon College sponsor and are subject to a security review.
6. Third parties must be made aware and must comply with all applicable Clarendon College policies, practice standards, agreements, and guidelines, including but not limited to:
 - a) Acceptable Use Policy
 - b) Digital Encryption Policy
 - c) Privacy Policy
 - d) Network Access Policy
 - e) Portable Computing Policy
 - f) Change Management Policy
 - g) Clarendon College Information Security Program

7. Third-party agreements and contracts must specify:
 - a) The Clarendon College information to which the third party has access.
 - b) How Clarendon College information is to be protected by the third party.
 - c) Acceptable methods for the return, destruction, or disposal of Clarendon College information in the third party's possession at the end of the contract.
8. Third parties must only use Clarendon College information and information technology resources for the business agreement.
9. Any other Clarendon College information acquired by the third party during the contract cannot be used for the third party's purposes or divulged to others.
10. Third-party personnel must report all security incidents immediately to the appropriate Clarendon College sponsor and the Information Security Officer (ISO).

Any third-party account holder who violates this policy will have the account suspended, and the account holder's sponsor will be notified. Following a review, Clarendon College will implement the actions specified by the ISO to reinstate or remove the account.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
User Accounts Password Policy:

PURPOSE:

Strong and confidential passwords will protect all user accounts. Users will protect the security of those passwords by managing passwords according to Clarendon College-IT password procedures.

System and Application Administrators will ensure account passwords are secured using state and federal guidelines and industry best practices.

SCOPE:

The Clarendon College User Accounts Password policy applies equally to all individuals granted access privileges to any Clarendon College information technology resources.

POLICY:

Users are responsible for what is accessed, downloaded, or created under their credentials, regardless of intent. An unauthorized person can cause a loss of information confidentiality, integrity, and availability that may result in liability, loss of trust, or embarrassment to Clarendon College.

Account holder's responsibilities:

1. Must create a strong password and protect it.
2. The password must have a minimum length of eight (14) alphanumeric characters.
3. Password must contain a mix of upper case, lower case, and numeric characters and special characters (!@#%^&*+=?/~';:,<>|\).
4. Passwords must not be easy to guess; for instance, they should not include part of your social security number, birth date, nickname, etc.
5. Passwords must not be easily accessible to others (e.g., posted on monitors or under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. Clarendon College username and password should not be used for external services (e.g., LinkedIn, Facebook, or Twitter).
9. Users should never share passwords with anyone, including family, supervisors, co-workers, and Clarendon College IT personnel.

10. Users must change passwords at least once every 365 days, reference NIST SP-800-63 ([NIST Password Guidelines](#) | [AuditBoard](#)).
11. If you know or suspect your account has been compromised, change your password immediately and contact Clarendon College-IT for further guidance and assistance.
12. If Clarendon College-IT suspects your account has been compromised, your account will be deactivated, and you will be contacted immediately.
13. Employees must use Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) with their network and PC access passwords. Student use of 2FA/MFA is also encouraged.
14. Recording login information on paper notes or other unsecured means is prohibited. Using electronic password managers to store and record user login credentials is highly encouraged and is available.

Any individuals responsible for managing passwords must:

1. Prevent or take steps to reduce the exposure of any clear text or unencrypted account passwords that Clarendon College applications, systems, or other services have received for authentication purposes.
2. Never request that passwords be transmitted unencrypted. Passwords must never be sent via unsecured email. If email is used to transmit login information, it must be sent via a secure email process.
3. Never circumvent this password policy for ease of use.
4. Coordinate with Clarendon College-IT regarding password procedures.

DEFINITIONS:

Clarendon College IT: Individuals or contractors that work or perform duties on behalf of the Clarendon College IT Department.

Compromised Account: The unauthorized use of a computer account by someone other than the account owner.

Encrypted: The conversion of data into a form called cipher text that unauthorized people cannot easily understand. Encryption is achieved using Windows native Bit Locker or other available software.

Password: A string of characters input by a system user to substantiate their identity, authority, and access rights to the computer system they wish to use.

System Administrator: Individual(s) responsible for running/operating systems daily.

Multi-Factor Authentication (MFA): is a security measure that requires more than one form of identification to log in to an account. It's also known as two-step verification.

Two-Factor Authentication (2FA): an identity and access management security method that requires two forms of identification to access resources and data. 2FA allows businesses to monitor and help safeguard their most vulnerable information and networks.

Secure Email Services: Secure email services use encryption and identity checks to protect your messages. Some of the most secure email providers include Mimecast, Barracuda, and Proton.

Unauthorized person: A person without official permission or approval to access Clarendon College systems.

Password Manager: is a software program that stores and manages passwords for online accounts. It can also generate strong passwords and automatically fill in forms, i.e., Keeper.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at

<https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on February 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 13, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
User Accounts Password Policy:

PURPOSE:

Strong and confidential passwords will protect all user accounts. Users will protect the security of those passwords by managing passwords according to Clarendon College-IT password procedures.

System and Application Administrators will ensure account passwords are secured using state and federal guidelines and industry best practices.

SCOPE:

The Clarendon College User Accounts Password policy applies equally to all individuals granted access privileges to any Clarendon College information technology resources.

POLICY:

Users are responsible for what is accessed, downloaded, or created under their credentials, regardless of intent. An unauthorized person can cause a loss of information confidentiality, integrity, and availability that may result in liability, loss of trust, or embarrassment to Clarendon College.

Account holder's responsibilities:

1. Must create a strong password and protect it.
2. The password must have a minimum length of eight (14) alphanumeric characters.
3. Password must contain a mix of upper case, lower case, and numeric characters and special characters (!@#%^&*+=?/~';:,<>|\).
4. Passwords must not be easy to guess; for instance, they should not include part of your social security number, birth date, nickname, etc.
5. Passwords must not be easily accessible to others (e.g., posted on monitors or under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. Clarendon College username and password should not be used for external services (e.g., LinkedIn, Facebook, or Twitter).
9. Users should never share passwords with anyone, including family, supervisors, co-workers, and Clarendon College IT personnel.

10. Users must change passwords at least once every 365 days, reference NIST SP-800-63 ([NIST Password Guidelines](#) | [AuditBoard](#)).
11. If you know or suspect your account has been compromised, change your password immediately and contact Clarendon College-IT for further guidance and assistance.
12. If Clarendon College-IT suspects your account has been compromised, your account will be deactivated, and you will be contacted immediately.
13. Employees must use Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) with their network and PC access passwords. Student use of 2FA/MFA is also encouraged.
14. Recording login information on paper notes or other unsecured means is prohibited. Using electronic password managers to store and record user login credentials is highly encouraged and is available.

Any individuals responsible for managing passwords must:

1. Prevent or take steps to reduce the exposure of any clear text or unencrypted account passwords that Clarendon College applications, systems, or other services have received for authentication purposes.
2. Never request that passwords be transmitted unencrypted. Passwords must never be sent via unsecured email. If email is used to transmit login information, it must be sent via a secure email process.
3. Never circumvent this password policy for ease of use.
4. Coordinate with Clarendon College-IT regarding password procedures.

DEFINITIONS:

Clarendon College IT: Individuals or contractors that work or perform duties on behalf of the Clarendon College IT Department.

Compromised Account: The unauthorized use of a computer account by someone other than the account owner.

Encrypted: The conversion of data into a form called cipher text that unauthorized people cannot easily understand. Encryption is achieved using Windows native Bit Locker or other available software.

Password: A string of characters input by a system user to substantiate their identity, authority, and access rights to the computer system they wish to use.

System Administrator: Individual(s) responsible for running/operating systems daily.

Multi-Factor Authentication (MFA): is a security measure that requires more than one form of identification to log in to an account. It's also known as two-step verification.

Two-Factor Authentication (2FA): an identity and access management security method that requires two forms of identification to access resources and data. 2FA allows businesses to monitor and help safeguard their most vulnerable information and networks.

Secure Email Services: Secure email services use encryption and identity checks to protect your messages. Some of the most secure email providers include Mimecast, Barracuda, and Proton.

Unauthorized person: A person without official permission or approval to access Clarendon College systems.

Password Manager: is a software program that stores and manages passwords for online accounts. It can also generate strong passwords and automatically fill in forms, i.e., Keeper.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at

<https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on February 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 13, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
User Account Credentials Management Policy:

PURPOSE:

This policy establishes standards for administering user account credentials that access Clarendon College's information technology resources. These resources must be protected from unauthorized access, loss, corruption, or destruction, thus ensuring these resources' confidentiality, integrity, and availability. Proper management of account credentials provides a means of assuring accountability and protecting Clarendon College's resources. The standards established in this policy include issuing account credentials, granting access to approved resources, account credential maintenance, and deactivation processes.

Scope:

The Clarendon College User Account Credentials Management policy applies to those responsible for managing user account credentials on Clarendon College's information technology resources.

Policy Statement:

Creating unique domain user account credentials is an automated process utilizing the current approved Clarendon College account naming convention and is based on assigned roles within the Enterprise Resource Planning (ERP) system (e.g., faculty, staff, student worker, student, visitor, alums, etc.) The level of authorized access will be based on the principle of least privilege (PoLP), but if a user is assigned multiple roles, the most privileged role will take precedence.

1. Creating a user account credential issues, a unique, non-transferable electronic identity known as the "username" and a corresponding "password." Usernames will remain in effect throughout the individual's official affiliation with Clarendon College. (User Account Password Policy).
2. Usernames are not reused.
3. When an individual changes role or ends their affiliation, Clarendon College-IT deactivates the user account credentials that no longer meet Clarendon College's eligibility requirements (User Account Management Policy) and removes non-standard access.
4. Upon user activation, account holders can access the resources their role membership dictates.
5. Clarendon College-IT requires users to change passwords per the User Account Password Policy.
6. Requests for exceptions to this policy must be submitted in writing (Clarendon College-Compliance Policy and Exception Form) to the Information Security Officer (ISO) or Vice President of Information Technology. They will be reviewed on a case-

by-case basis. Requests shall be justified, documented, and communicated during the risk assessment.

Definition:

Enterprise Resource Planning (ERP): is a software system that helps businesses manage their core processes, such as accounting, procurement, and supply chain. ERP systems can improve efficiency and decision-making.

Principle of Least Privilege (PoLP): is an information security concept that maintains that a user or entity should only have access to the specific data, resources, and applications needed to complete a required task.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 18, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Web Privacy and Site Link Statement:

Web Privacy Policy

Clarendon College has created this privacy statement to demonstrate our firm commitment to privacy. Our information gathering and dissemination practices for this website are the following disclosures: www.clarendoncollege.edu. This site contains links to other sites. Clarendon College (www.clarendoncollege.edu) is not responsible for privacy practices or the content of Websites outside of Clarendon College's control.

We may use your IP address to help diagnose problems with our web server and to administer our Web site. Our site uses forms for students, faculty, staff, and visitors to request information, products, and services. We collect contact information (like email addresses) and unique identifiers (like social security numbers) for college business, such as college registration and/or catalogs sent to potential students.

We use cookies to collect information for collective analytics or tracking student progression within our learning management system. Individual data is not harvested. (Note: A cookie file contains unique information a website can use to track such things as passwords, lists of pages you've visited, and the date when you last looked at a specific page or to identify your session at a particular website.)

Please send us an electronic mail message with a question or comment that contains personally identifying information or fill out a form that e-mails us this information. We will only use the personally identifiable information to respond to your request and analyze trends. We may redirect your message to another government agency or person in a better position to answer your question.

For site management functions, information is collected for analysis and statistical purposes. This information is not reported or used in any manner that would reveal personally identifiable information and will not be released to any outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

Public Forums

This site makes available chat rooms, forums, message boards, and/or news groups. Please remember that any information disclosed in these areas becomes public, and you should exercise caution when disclosing your personal information.

For Additional Information

Additional information regarding privacy and security policies is provided in the Privacy and Security Policy Guidelines at <http://www.dir.state.tx.us/standards/srrpub11-privacy-policy.htm>. The U.S. Federal Trade Commission also provides information for educating consumers and businesses about the importance of personal information privacy at <http://www.ftc.gov/privacy/>.

Contacting the Web Site

If you have any questions about this privacy statement, the practices of this site, or your dealings with this Web site, you can contact

Web Admin

Clarendon College

P.O. Box 968

Clarendon, TX 79226

administrator@clarendoncollege.edu

Web Linking

Clarendon College complies with the State Web Site Link and Privacy Policy at http://www.dir.state.tx.us/standards/link_policy.htm. Clarendon College encourages organizations that link to this Website to comply with the provisions of the State Web Site Link and Privacy Policy, especially regarding the protection of the privacy rights of individuals, and to make reasonable efforts to provide accessible sites.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Web Site Disclaimer Statement:

The Clarendon College website, <http://www.clarendoncollege.edu>, is provided as a public service. Users of this website are responsible for checking the accuracy, completeness, currency, and/or suitability of all information. Clarendon College makes no representations, guarantees, or warranties regarding the accuracy, completeness, currency, or suitability of the information provided via this website.

This Web site provides links to other Web sites, both public and private, for informational purposes. Clarendon College expressly disclaims any liability and responsibility for any claims or damage that may arise as a result of Clarendon College providing the Website or the information it contains or that may occur in any way concerning any Websites maintained by third parties and linked to the Clarendon College site. Clarendon College advises site visitors to read the privacy policies of any third-party sites accessed through this site.

Including links from this site does not imply endorsement by the Clarendon College. Specific questions regarding a document should be directed to the appropriate organization. Clarendon College makes no effort to verify independently and does not exert editorial control over information on pages outside the www.clarendoncollege.edu domain.

Clarendon College does not collect or track personal information from website visitors. Generic information from server logs may be used to track the number of hits to the site and determine what types of browser software visitors use. This information will be used only in aggregate form to improve website design. Please review the Clarendon College Privacy Statement for details.

Clarendon College does not endorse any products, vendors, consultants, or documentation referenced on this website. Any mention of vendors, products, or services is for informational purposes only.

Related Policies, References and Attachments:

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at <https://www.clarendoncollege.edu/information-technology>. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on _____, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.

Ratify New Hires/Resignations/ Appointments/
Reassignments & Other Personnel Matters



CLARENDON COLLEGE

RECOMMENDATION FOR EMPLOYMENT

TO: President, Clarendon College

DATE: 3/13/2025

I recommend Lexie Blackburn to be employed in
the position of Administrative Assistant to the Vice President
starting April 1, 2025 or for a specific period of time
starting on _____ and ending on _____.

I have complied with the guidelines and policies of Clarendon College for selection of the above
named person. The number of applicants that were considered for the above named position
was 2. I consider the above named person to be the best qualified of all applicants
because: (State reasons why the person recommended is the best qualified)
Met requirements for position.

FUNDING SOURCE: ☐ Institutional Funds ☐ Grant/Other Funds _____

SALARY & SPECIAL CONTRACT CONDITIONS:
\$34,200 per year.

SALARY ACCOUNT: 21-3010-01-10-5840

Recommended By: Brad Vanden Brogaard
Date: 3-14-25

Approved: Texas D. Tap Buckhauser
Date: March 14, 2025

Acknowledged By: Cindy Upton
Cindy Upton Mar 14, 2025 11:08 CDT

Date: _____











Recommendation for Employment - Lexie Blackburn

Final Audit Report

2025-03-14


Created:	2025-03-13
By:	Evie Wright (evie.wright@clarendoncollege.edu)
Status:	Signed
Transaction ID:	CBJCHBCAABAA01E_kVF9bcXmluPc8AFS_rl3vbBGtXIg


"Recommendation for Employment - Lexie Blackburn" History

-  Document created by Evie Wright (evie.wright@clarendoncollege.edu)
2025-03-13 - 1:07:43 PM GMT - IP address: 209.40.172.170
-  Document emailed to Brad Vanden Boogaard (brad.vandenboogaard@clarendoncollege.edu) for signature
2025-03-13 - 1:08:39 PM GMT
-  Email viewed by Brad Vanden Boogaard (brad.vandenboogaard@clarendoncollege.edu)
2025-03-13 - 8:57:57 PM GMT - IP address: 172.225.216.114
-  Document e-signed by Brad Vanden Boogaard (brad.vandenboogaard@clarendoncollege.edu)
Signature Date: 2025-03-14 - 3:26:57 PM GMT - Time Source: server- IP address: 209.40.172.170
-  Document emailed to Texas Buckhaults (TEX.BUCKHAULTS@CLARENDONCOLLEGE.EDU) for signature
2025-03-14 - 3:26:59 PM GMT
-  Email viewed by Texas Buckhaults (TEX.BUCKHAULTS@CLARENDONCOLLEGE.EDU)
2025-03-14 - 4:01:00 PM GMT - IP address: 172.226.178.5
-  Document e-signed by Texas Buckhaults (TEX.BUCKHAULTS@CLARENDONCOLLEGE.EDU)
Signature Date: 2025-03-14 - 4:04:47 PM GMT - Time Source: server- IP address: 172.59.192.148
-  Document emailed to cindy.upton@clarendoncollege.edu for signature
2025-03-14 - 4:04:49 PM GMT
-  Email viewed by cindy.upton@clarendoncollege.edu
2025-03-14 - 4:05:25 PM GMT - IP address: 209.40.172.170
-  Signer cindy.upton@clarendoncollege.edu entered name at signing as Cindy Upton
2025-03-14 - 4:06:21 PM GMT - IP address: 209.40.172.170



Adobe Acrobat Sign

 Document e-signed by Cindy Upton (cindy.upton@clarendoncollege.edu)
Signature Date: 2025-03-14 - 4:06:23 PM GMT - Time Source: server- IP address: 209.40.172.170

 Agreement completed.
2025-03-14 - 4:06:23 PM GMT

Morgan De La Cruz
morgan.delacruz.312@gmail.com
806.670.0738
March 11, 2025

Dear Clarendon College, CC Cosmetology Department, and all associated parties,

I am writing to formally resign from my position as Dual Credit Cosmetology Instructor at Clarendon Cosmetology Pampa Campus, effective May 16, 2025 - the end of the Spring 2025 Semester.

This decision was not an easy one, and it comes after careful consideration of my personal and professional goals. I want to express my sincere gratitude for the opportunity to work with this team. My time at Clarendon College Cosmetology has been incredibly rewarding, and I have greatly appreciated the opportunities for growth and development that I have been given during my time here. The positive impact my students have made on me sits deep within my heart and is something I will carry with me always.

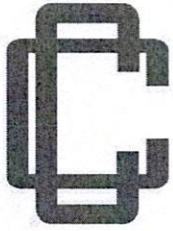
Please let me know how I can assist in the transition process over the coming weeks. I am committed to making this transition as smooth as possible for everyone involved. Thank you once again for the opportunity to be a part of the bulldog family and I look forward to always being able to partner with the Clarendon College Cosmetology in future classes, demos, projects etc.

I wish everyone at Clarendon College continued success in the future.

Sincerely,
Morgan De La Cruz



Reports on Non-Action Items



CLARENDON COLLEGE

www.clarendoncollege.edu

MEMORANDUM FOR THE CLARENDON COLLEGE FACULTY 2023-2024

FROM: CC FACULTY SENATE

SUBJECT: 21 February 2025, Meeting Agenda

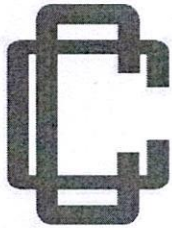
1. The Clarendon College Faculty Senate will convene via teleconference on March 28 at 1205p for the ZOOM meeting is 806-874-4816
2. Opening Business
 - o Call to Order -Roll Call
3. Roll Call (or distribute attendance sheet)

Name		Present/Absent	Proxy Given to
Chair Caraway	Dr. Edward	P	
Vice Chair Wiginton,	Larry	P	
Secretary, Swygard	Dr. Brad	P	
Sentinel Thompson	Bethany	P	
Clarendon Campus			
Adams	Austin	P	
Broom	Toni		
Chesser	Tye	P	
Cranfield	Elizabeth		Beth
Donahue	Dr. Rodney		ken
Hatfield	Stacy		
Hunter	Alicia		
James	Mark		
Jeffrey	Kim		Tye
Johnson	Krystal		
McBeth	Natasha		
McIntosh	Dr. Ken	P	
McLatchy	Andy	P	
Miller	Cindie		
O'Neal	Debra		
Owens	Barbara		

P.O. Box 968 | Clarendon, Texas 79226 | 1.800.687.9737 | T 806.874.3571 | F 806.874.3201

1601 W. Kentucky | Pampa, Texas 79065 | T 806.665.8801 | F 806.665.0444

1902 Ave. G NW Suite 1A | Childress, Texas 79201 | T 940.937.2001 | F 940.937.2520



CLARENDON COLLEGE

www.clarendoncollege.edu

Paul	Dr. Laura	P	
Randall	Rachel	P	
Sain	Dr. Jeremy	P	
Sain	Roberta	P	
Snook	Kregg		
Treichel	Johnny	P	
Pampa Center			
Bennett	Ryan		
Caraway	Dr. Edward		
Carreon-Jimenez	Araceli		
Denham	Sherrie		Ed?
Hunter	Alicia		
McBeth	Natasha		
McKinney	Ashley		
McLatchy	Andy		
Noud	Katherine		
ONeal	Debra		
Simmons	Mark		
Tandy	William		
Upton	Casey		
Vance	Frank		
Watson	Darla		
Amarillo Center			
Hatfield	Stacy		
Johnson	Krystal		
Seal	Amie		
LRC/Library			
Reed	Pamela	P	
Schmidt	Tammi	P	

4. Adopt Today's Agenda YES/NO:

- Motion to adopt: Beth Thompson
- Second: Dr. Sain

P.O. Box 968 | Clarendon, Texas 79226 | 1.800.687.9737 | T 806.874.3571 | F 806.874.3201

1601 W. Kentucky | Pampa, Texas 79065 | T 806.665.8801 | F 806.665.0444

1902 Ave. G NW Suite 1A | Childress, Texas 79201 | T 940.937.2001 | F 940.937.2520



CLARENDON COLLEGE

www.clarendoncollege.edu

5. Approve Minutes of Previous Meeting
 - Approved by: Beth Thompson
 - Second: Elizabeth Cranford
6. Reports:
 - NSLS Zoom Event
7. Unfinished Business:
8. New Business:
 - Artificial Intelligence Usage Policy
 - Scheduling and Move-In dates
 - Dual Credit Spring Break Differences
 - Notice of Faculty Senate Nominations
 - Referring struggling students to Charlta and Tamara
9. Other Business
10. Adjournment (time end):
 - Moves to adjourn the meeting: Dr. Sain
 - Second: Dr. Swygard

Minutes for the February meeting

Bethany Thompson reported on the NLS zoom event.

Mr. Vanden Boogaard noted that Clarendon College's SACSCOC report has been submitted. This is the first step in our accreditation review process.

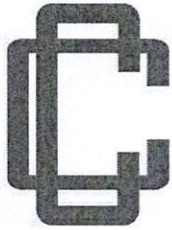
There was discussion concerning the January move-in date and the fact that with Dr. Martin Luther King Jr. Day follows and creates some issues. Quite a few of the teams come in before the cafeteria opens. It was stated that the calendars can be modified in the future. The Senate voted to direct the executive committee to meet with Mr. Vanden Boogaard regarding the calendar.

Charlta King and Tamara Bains noted that referral of struggling students was being utilized, and that the faculty should keep using it to encourage and improve student success.

P.O. Box 968 | Clarendon, Texas 79226 | 1.800.687.9737 | T 806.874.3571 | F 806.874.3201

1601 W. Kentucky | Pampa, Texas 79065 | T 806.665.8801 | F 806.665.0444

1902 Ave. G NW Suite 1A | Childress, Texas 79201 | T 940.937.2001 | F 940.937.2520



CLARENDON COLLEGE

www.clarendoncollege.edu

The State of Texas has directed schools to have an Artificial Intelligence Use policy that does not impede students with accommodations. Mr. Will Thompson has provided information that the faculty should read and understand and establish a policy in our classrooms consistent with it.

There are differences this year between the Spring Break of Clarendon College and several of the High Schools with Dual-Credit students. The consensus was that they were still responsible for their college work. However, each faculty member could manage it how they see fit.

An impromptu discussion about moving to a four-day week came up. Some of the secondary schools in the area are moving towards a four-day week. It was noted that this has been discussed before and advanced to the administration.

Mr. Lary Wiginton gave a brief report from the Board of Regents meeting.

Notification was given that nominations for Faculty Senate officers are coming up.

Dr. Brad Swygard
Faculty Senate Secretary