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 mostly 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 datacenter. The Austin facility boasts a Tier IV datacenter rating which is the highest achievable.

The Run Biz datacenter 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 datacenter to a local set of disks.
2. Each evening all backups are copied offsite to the Las Vegas datacenter. The LV datacenter is equipped with standby disaster recovery hardware. Should a catastrophic event result in the loss of the Austin datacenter, all Runbiz servers can be recovered to the previous night's backup. The servers can then be brought online in the Las Vegas datacenter. College wide access can be restored in 24 to 48 hours. See Appendix A and C for diagram explanations of the process.
3. See 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) Academic Vice President, academic records lead,
        3) Business Manager, purchasing and insurance lead,
        4) Vice President of IT, systems management lead,
        5) Director of Maintenance, facilities lead,
        6) In addition, site assistance member, depending on the location of disaster.
        7) Other staff members as deemed necessary at the time of the disaster.
    b. All members of the Disaster Response team will be contacted in the above order as soon as possible.

c. During a disaster a communications channel will be opened to 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. If communications have been affected, the college's Internet and phone service providers will be contacted.
    1) Campus or Center ISP service provider
        i. Main Campus/Childress and Amarillo, AMA Techtel
        ii. Pampa Center, CableOne
        iii. Childress Center, Santa Rosa Communications
    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 a listing of all major IT vendors for Clarendon College and their contact numbers.

5. Critical Systems:
    a. CAMS Enterprise
    b. Dynamics GP – ERP / Accouting 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 latest recoverable restore point on the backup appliance
    b. Initialize recovery wizard
    c. Select "Volume Restore"
    d. Select Hyper-V host as destination
    e. Keep original Resources levels
    f. Initialize Recovery
    g. Once VM is online, perform a test login to the operating system
    h. Confirm system is online with a route to the internet
    i. Configure firewall to allow access back to the internal server
2. PC's, Internet, network, and phone services will be reallocated and restored according to the following areas and or prioritize 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:
If possible, for quickest possible restoration, old PC and servers will be made operational until new systems can be ordered and deployed.

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 that has the responsibility for maintenance and supervision of the Clarendon College IT infrastructure.

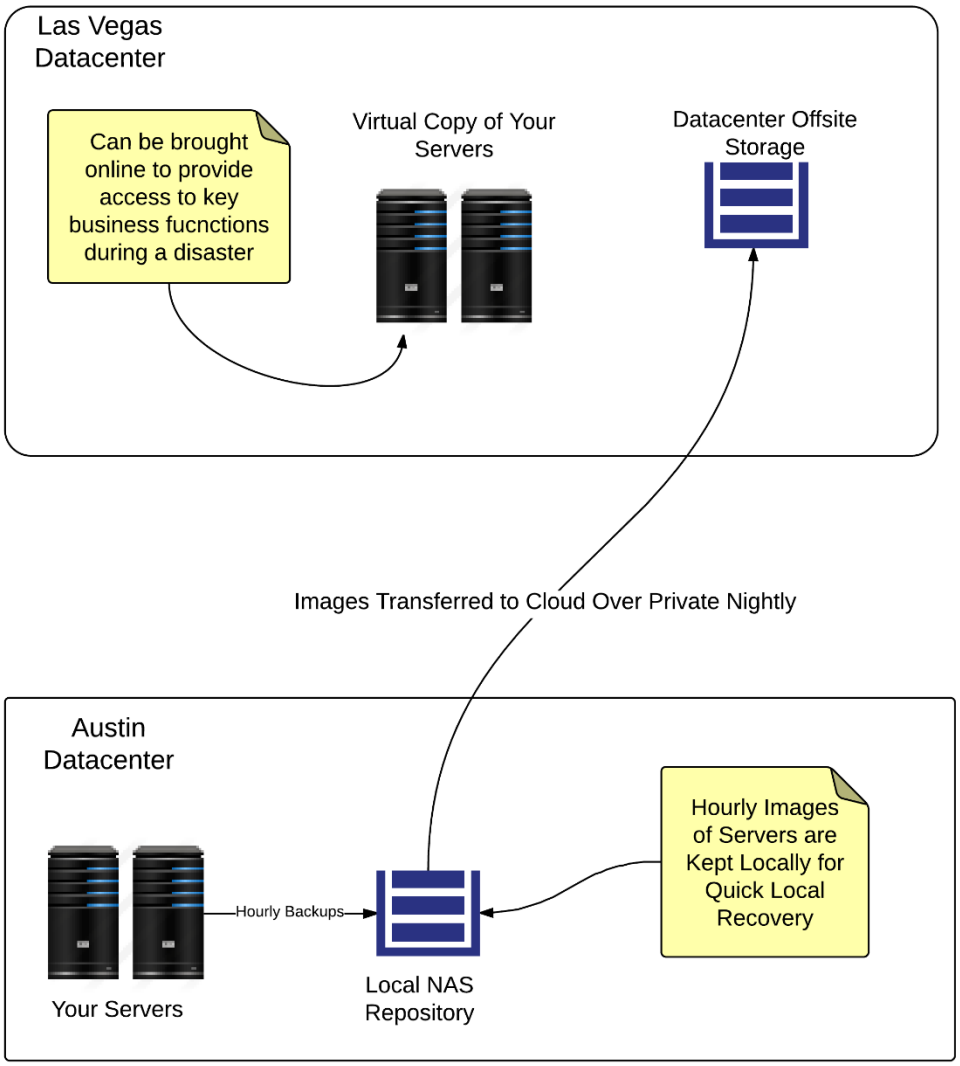
Cloud Storage: A service model in which data is maintained, managed and backed up remotely and made available to users over the Internet.

Related Policies, Reference s 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.
Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. 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 [Date], version1.1 as of July 15, 2023. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.

APPENDIX A.

Offsite Backup:
The below diagram depicts the backup methodology from Austin to Las Vegas



This policy was approved by the Clarendon College Board of Regents on [Date], version1.1 as of July 15, 2023. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.

APPENDIX B.

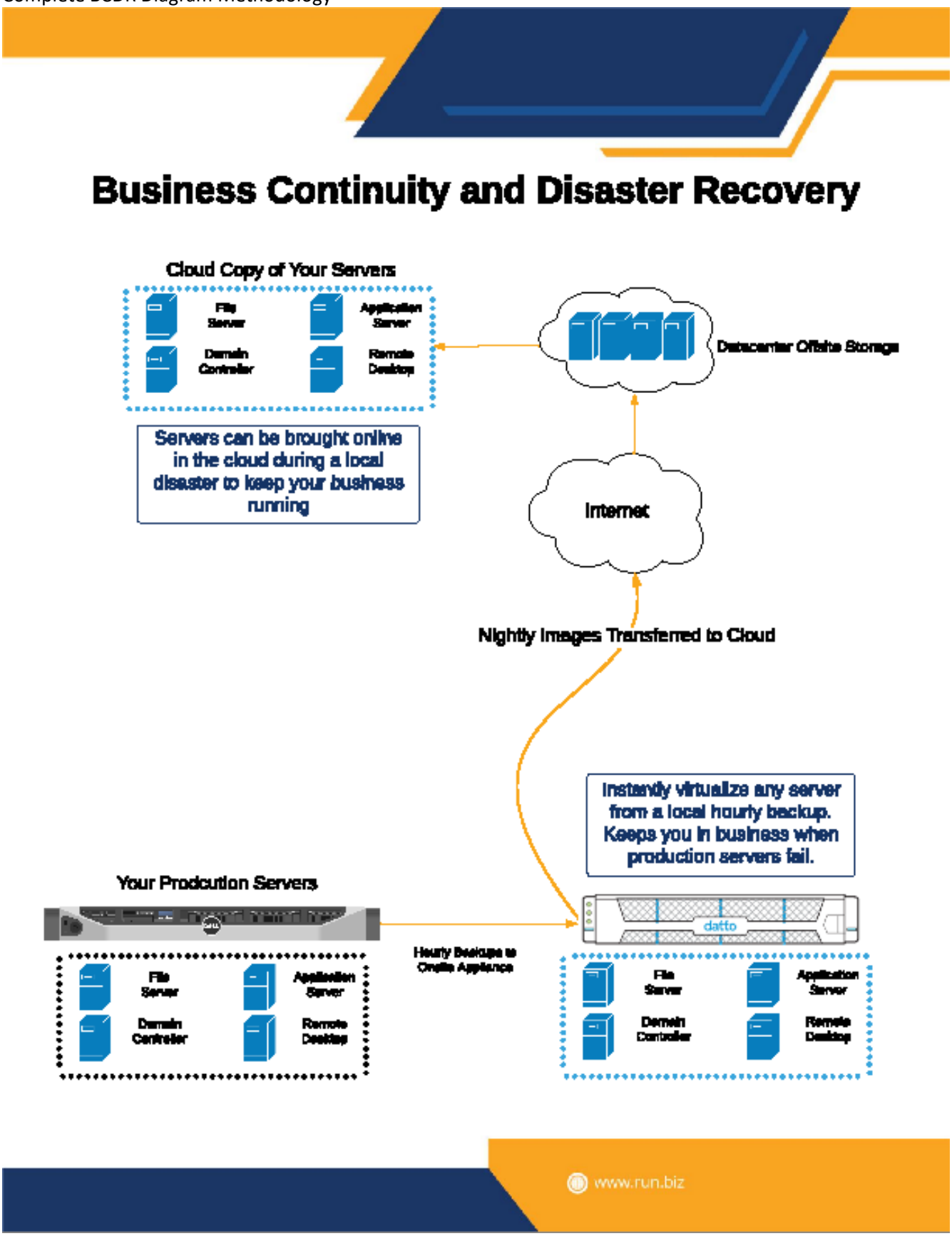
Vendor phone listing.

Agency	Area of Operation	Phone Number
Run Biz	General Tech Support	806-322-2150
AMA Techtel	Internet Provider, (AM, CC, CH)	806-322-2222
AMA Techtel	Phone Provider (AM, CC, PA)	806-322-2222
Cable One	Internet Provider (PA)	877-469-2251
Santa Rosa	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	

This policy was approved by the Clarendon College Board of Regents on [Date], version1.1 as of July 15, 2023. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.

Appendix C.

Complete BCDR Diagram Methodology



This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.