

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

PURPOSE:

The purpose of this policy is to provide a set of measures that will mitigate information security risks associated with IT Administrators/Special Access.

IT Administrators/Special Access is defined as users that have 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 information technology resources. In order to safeguard information technology resources, the following controls are required:

1. All users of Administrative/Special Access accounts must have account-management instructions, documentation, and authorization.
2. All users must sign the Clarendon College Non-Disclosure Agreement and be current on their annual Cybersecurity Awareness Training.
3. Each individual who uses special access accounts must use the account privilege most appropriate with work being 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 as to whether it should remain a shared account or not. (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 gain access to the administrator account in an emergency situation.

7. When special access accounts are needed for audit, software development, software installation or other defined need, special access must be:
 - a. Authorized by the system owner, Information Resource Manager, or Information Security Officer. (E.g., Clarendon College-IT is the system owner for 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 to the State of Texas to manage Clarendon College information technology resources.

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

IT Administrators/Special Access: users that have elevated account privileges that 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 in order to minimize the potential impact of a threat.

Non-Disclosure Agreement (NDA): Formal acknowledgement that all employees must sign acknowledging they have read and understand SPC requirements regarding computer security policies and procedures. This agreement becomes 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>.

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 July 17, 2023, version 1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.