

Administrator/Special Access Policy

<http://pvamu.edu/pages/2532.asp>

1. General

Information Technology Services support staff, system administrators and others may have special access account privilege requirements compared to the access privileges of typical users. Administrator accounts and other special access accounts have extended and overarching privileges in comparison with typical user accounts, thus the granting, controlling and monitoring of these accounts is extremely important to an overall security program.

2. Applicability

This procedure applies to all University information resources. The purpose of this procedure is to provide a set of measures that will mitigate information security risks associated with Administrators Special Access. The intended audience for this procedure includes, but is not limited to, all information resources data/owners, management personnel, system administrators, and end users.

3. Definitions

- **Information Resources (IR):** the procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.

4. Procedures

1. Each individual that uses administrator/special access accounts shall refrain from abuse of privilege and shall only conduct investigations as directed by appropriate University management personnel.
2. In those cases where law enforcement agencies request access in conjunction with an investigation, the request shall be in writing (e.g., subpoena, court order). All such requests shall be reported to the appropriate department head, director, or their designee before any action is taken.
3. Each individual that uses administrator/special access accounts shall use the account or access privilege most appropriate for the requirements of the work being performed (e.g., user account vs. administrator account).
4. The password for a shared administrator/special access account shall change under the following conditions:
 - a. an individual knowing the password leaves the University or department;
 - b. job duties change such that the individual no longer performs functions requiring administrator/special access;
 - c. a contractor or vendor with such access leaves or completes their work.
5. In the case where a system has only one administrator, there shall be a password stored in a secure space (safe or vault) in an envelope such that an appropriate individual other than the administrator can gain access to the administrator account in an emergency situation.
6. When special access accounts are developed for internal or external audits, software development, software installation, or other defined needs, they must be:
 - a. authorized by a department head;
 - b. created with a specific expiration date; and,
 - c. removed when the task or project is complete.