Privileged Access Policy

Summary

Privileged access, commonly referred to as supervisor, administrator, admin, or root access, allows an individual full permissions to the resources within their authority. Granting various levels of privileged access to systems administrators, network administrators, database administrators, application developers, and desktop support staff is standard practice. An administrator may have access to network devices, file servers, user accounts and user data, financial and personnel data, or desktop operating systems.

Purpose

This policy informs administrators at all levels of the inherent obligations and responsibilities that accompany privileged access.

Policy

- Privileged access is only granted to authorized individuals
- Users with privileged access will have two user IDs: one for normal day-to-day activities and one for performing administrator duties.
- Administrators may only use their administrator account to perform administrator functions.
- Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.

Violation of this policy and procedures stated within including not meeting deadlines of procedures by personnel listed will be reported to the CIO and appropriate actions taken.

Procedures and Responsibilities

- Users may request privileged access from the Information Security Officer. Substantial justification is required for approval. The appropriate Administrator is responsible for creating the privileged account. All normal user ID and password polices and procedures apply.
- Users with privileged access have a responsibility to protect the confidentiality of any information they encounter while performing their duties.
- Users with privileged access are responsible for complying with all applicable laws, regulations, policies, and procedures.
- Users with privileged access must always be aware that these privileges place them in a position of considerable trust. Users must not breach that trust by misusing privileges or failing to maintain a high professional standard.
- Trusted Administrators will work with their IT Directors to create and provide a non- electronic list of all privileged user accounts to the Information Security

Officer of critical system network devices, file servers, user accounts and user data, financial and personnel data, or desktop operating systems.

- A time of two weeks will be allotted for the gathering and producing of the non-electronic lists by the Administrators to the IT Directors
- IT Directors will meet with the Information Security Officer and provide the non-electronic lists of privilege accounts and passwords.
- This meeting will take place within 3 days after the IT Directors have obtained the non-electronic lists from the Administrators.
- The Information Security Officer will create a master list from the collected departmental privileged user account lists and store on a CD\DVD inside predetermined IT vaults.
- The CD\DVD will be created and stored in the It vault no later than 3 days after the meeting has occurred between the IT Directors and the Information Security Officer.
- There will be a bi-annual (every six months) privileged user account audit performed by the Directors at the request of the Information Security Officer to verify account credibility and to change the passwords on the existing privileged user accounts.
- Making any updates, additions, or deletions of privilege user accounts and\or passwords requires the notification and approval by one of the following IT Director, Information Security Officer, or CIO.
- Immediately following any updates, additions, or deletions to the privilege user accounts and\or passwords the IT Director or CIO will contact the Information Security Officer to update the master list.

Related USG Policy

3.1 (IT Handbook) Information System User Account Management & 5 (IT Handbook) Information Security

Last Update

4/17/2014

Responsible Authority

Chief Information Security Officer