Standards for Individuals with Privileged Access [1]

Privileged access is typically granted to university staff, IT administrators, and other users whose job duties require special privileges to access university information. These standards apply to all University servers that are used to maintain university information. Individuals with privileged access to workstations or mobile devices that maintain private information must also comply with these standards.

Definitions

Access - The ability or the means necessary to read, write, modify, or communicate data/information or otherwise instruct or use any IT resource.

Privileged Access - Privileged access are rights to computer or application systems that have been granted to an individual beyond that of a typical user that can bypass, modify, or disable technical or operational security controls. Examples may include the ability to install software; install or modify system processes; create or modify system configurations; create or modify system access controls; view or control the screen of the user through remote access technologies in order to assist them.

Standards

Departments who cannot meet this standard should consult with their respective Information Security Officer regarding alternative approaches.

Individuals with privileged access must understand that failure to comply with these standards may result in a loss of access or other disciplinary actions. Such a determination should be made by the employee's appointing authority in consultation with the appropriate campus Information Security Officer and the campus information oversight authority.

The below standards should be followed for proper compliance:

- Privileged Accounts
    - Passwords, or use of the privileged account, must not be shared.
    - Passwords must be changed immediately if compromised either intentionally or unintentionally.
    - All information gained by privileged access is protected and may not be given to any non-privileged user or to any other privileged user except as required to perform necessary work and approved by the relevant data owner.
    - Access will be restricted allowing only essential functions required for valid business needs or job requirements as approved by the appropriate data owner. In instances where there is a potential conflict of interest, the campus information oversight authority or their delegate will approve access.
    - Privileged access applies to a particular period of time and includes only specific

tasks. Time periods are based on the required tasks; the time period may be brief, such as one- time access, intermittent access, or longer. Privileged access will end at the close of the time period granted. Privileged access will be reviewed, re-verified, and authorized by the user, his or her manager, and the applicable data owner every time the user's job duties change, or annually.

- Privileged access should not be used for day-to-day activities such as web browsing or reading email.
- Individuals with privileged access must respect the privacy of system users, respect the integrity of systems and related physical resources, and comply with relevant laws and regulations.
- Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.
- Individuals with privileged access have an obligation to keep informed of procedures, business practices, policies and operational guidelines pertaining to the activities of their unit.
- Individuals with privileged access must be aware of, and follow, change control processes before making changes to production systems.
- All individuals who are granted privileged access must have appropriate training for the relevant systems as well as have completed the Information Security for IT Service Providers training module. Individuals receiving privileged access must have received training prior to, or soon after, receiving privileged access. However, taking training after receiving privileged access is allowed only with the permission of the individual's supervisor. It is the supervisor's responsibility to consult with their campus Information Security Officer to understand the risks of allowing privileged access before receiving training.

Download Doc [2]

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/standards-individuals-privileged-access
[2] https://www.cu.edu/system/files/pages/243140-standards-individuals-privileged-access/docs/standards-indivuduals-privledged-access.docx