**Standards for individuals with privileged access**

Date of last review: 10/28/2014

**Background**

Because employees, contractors, and other affiliates with privileged access are able to modify systems or view highly confidential information, it is important to define this type of access and set standards to ensure such access is appropriately granted and utilized.  Privileged access is typically granted to system administrators, network administrators, staff who perform computing account-administration, or other staff whose job duties require special privileges to access University information. This document provides criteria for granting privileged access and requirements for monitoring such access. These standards apply to all systems that are used to maintain university information.  Departments who cannot meet this standard should consult with their respective Information Security Officer regarding alternative approaches

**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 - 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**

* When possible, full system administrator or "root" access will not be provided. Privileged access should use utilities that allow an application to run with privileged access (such as “sudo” on Unix and Linux based systems or “runas” or User Account Control on Microsoft Windows systems) or use role based access control within a database or application.
* 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 Chief Information Officer/Chief Technology Officer or their delegate will approve access.
* 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 (ISO) to understand the risks of allowing privileged access before receiving training.
* 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.
* Passwords, or use of the privileged account, must not be shared.
* Passwords must be changed immediately if thought to be compromised. System or service accounts should be unique to a specific business process so as to facilitate auditing.
* Systems will be configured to log all privileged access with an accurate timestamp. When feasible, logging should report actions taken by the privileged account.
* It is the responsibility for each unit to maintain documentation recording who has been granted privileged access to a specific system or class of systems. The Office of Information Security may request such documentation for periodic review or in response to a security incident.
* 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.
* Individuals with privileged access are required to follow the below guidelines when accessing social media websites/apps for official duties or in the conduct of official business:
* Conduct and ethics: As a representative of the university, it is imperative for you to maintain the same standards of conduct expected of all CU employees. Be respectful, positive, helpful and informative. Do not engage in negative banter and do not take a political stand on topics or legislation. https://www.cusys.edu/cuadvocates/cu-employee.html
* Protect highly confidential and proprietary information: Do not post any Highly Confidential, Confidential or sensitive information about the university and its students, staff, faculty or alumni. Types of Highly Confidential information include FERPA-protected student information, Social Security numbers, credit card numbers and medical records.
* Definitions for Highly Confidential, Confidential and sensitive information can be found on the Standards for Data Classification and System Security Categorization at http://www.cu.edu/ois/policies-and-resources
* Respect copyright and fair use. When posting, be mindful of the copyright and intellectual property rights of others and of the university. (Link to copyright info)
* Use appropriate branding: Do not use the university logo or any other university images or iconography on personal social media sites. Do not use the university’s name to promote a product, cause, or political party or candidate.
* Ensure the security of your social media account. A compromise of your account can lead to malicious entities posting inappropriate or even illegal material on your behalf. This could lead to reputational risk to the university. If you post on behalf to social media sites of the university be sure to use a different password for each your official social media accounts, personal social media accounts, and your university provided accounts. Follow best practices found at http://www.cu.edu/sites/default/files/Module05-Passwords-Newsletter.pdf in selecting and protecting your passwords. If you notice or hear about any abnormal activities occurring through your account or feel that it might have been compromised, contact the IT Security office.
* Terms of Services: Obey the Terms of Service of any Social Media platform employed.
* 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 ISO and the campus Chief Information Officer/Chief Technology Officer