Privileged Access Standard

Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, DBAs, staff performing computing account administration or other such employees whose job duties require special privileges over a computing system, application, database, or network.

Individuals with privileged access must respect the rights of the system users per the University’s Responsible Use of Information Technology policy, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices, and operational guidelines governing privileged access within their department.

In particular, the principles of academic freedom, freedom of speech, and privacy of information hold important implications for individuals with privileged access. They must comply with applicable policies, laws, regulations, precedents, and procedures while pursuing appropriate actions required to provide high-quality, secure, timely, and reliable computing services. The following general provisions apply.

GENERAL PROVISIONS

1. Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have read and signed the Access and Compliance Agreement.
2. Privileged access is reserved for employees performing their assigned job duties.
3. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.
4. Privileged access is used to perform standard system-related duties only on machines and networks whose responsibility is part of the employee's assigned job duties. Routine tasks (e.g., email, web browsing) not directly linked to the privileged access activity expose the resource to threats that would be greatly amplified by the level of privilege enjoyed by the operator. For this reason, they are prohibited. Examples of acceptable activity include:
   - installing system software;
   - relocating individuals’ files;
   - performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
   - running security checking programs;
   - monitoring the system to ensure reliability and security.
5. Privileged access is used to grant, change, or deny access to resources or privilege to another individual only for authorized account management activities; or under exceptional circumstances. Such actions must follow any existing organizational guidelines and procedures. Examples include:
   - disabling an account apparently responsible for serious misuse such as: attempting to compromise root (UNIX) or the administrator account (Windows), using a host to send harassing or threatening email, using software to mount attacks on other hosts, or engaging in activities designed to disrupt the functioning of the host itself;
   - accessing files for law enforcement authorities on the basis of a valid subpoena.
6. Accounts with elevated privileges will have the following prefixes depending on the type of account:
   - a_ Provide privileged access to an individual.
   - s_ Provide access to an application or service.
   - va_ Provide individual vendor privileged access.
7. Multi-Factor Access must be used when it is available for authentication to the subject resource.
8. Privileged accounts should only be accessed from university-owned and managed systems.

For any new or modified/upgraded applications that do not meet the requirements stated above, an exception must be requested by contacting the ITS Identity and Access Management Group.

This Standard is in support of the CIS Critical Controls.

Document sourced from https://security.berkeley.edu/model-privileged-access-agreement