University of CINCINNATI	*Policy Title:* **Privileged Access**	*Policy Number:* **9.1.14**
Category: Information Technology	**Effective Date:** 09/03/2021	**Policy Owner:** VP & CDO, Digital Technology Solutions
Policy applicable for: Faculty/Staff/Affiliates/ Student Workers	**Prior Effective Date:** 01/23/2019	**Responsible Office(s):** Office of Information Security

Background

Due to the operational knowledge and elevated access to sensitive University of Cincinnati (UC) information technology systems, individuals with Privileged or Administrative Access ("privileged access") are in a unique position of trust and responsibility. 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. Proper controls are required to mitigate this increased risk. Privileged access is typically granted to system administrators, network administrators, and staff performing system/computer account administration or other such employees whose job duties require special privileges over a computing system or network. A privileged access user could be a university employee, a contractor or vendor engaged by the university.

Policy

Privileged access users must use individual accounts with unique usernames and passwords that comply with the university's Password Policy. If there is a business need for shared credentials, an approved password storage system must be used. Access to the password storage system must be controlled by the university's approved multi-factor authentication.

Where technically feasible privileged access users must use the university approved privileged access management system.

The *Principle of Least Privilege* must be followed. Privileged access users must have permissions set to the lowest level of access needed to accomplish their job function. Standard university processes must be used to request and approve all privileged access accounts. Annual review of all privileged access is required.

Privileged access users should only have access on a *Need-to-Know* basis. The users

should only have access to, and knowledge of, the data needed to do their job function.

It is the responsibility of each business unit, to utilize a *Separation of Duties and Rotation of Duties* plan. Separation of duties is achieved by separating roles and responsibilities for a high-risk business process across multiple people. Rotation of Duties is achieved by rotating tasks periodically, so it becomes more difficult for users to collude together to engage in fraudulent behavior. These steps reduce risk to systems and university data, especially in situations where credentials become compromised.

Appropriate logs must be maintained in a centralized system where integrity and access can be controlled and monitored. Any additional logs must be made available to the Office of Information Security for review when requested. Logs shall be reviewed on a regular basis for malicious activity as required by university standards or regulatory compliance.

Privileged access users' desktop or laptop computers must be university owned and must be managed by centralized university-controlled endpoint technologies. When utilizing privileged access to university systems, users must, when technically feasible, connect via the university's physical network or use the universities VPN. Privileged access users must also use multi-factor authentication where technically feasible.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with all relevant laws, policies and regulation. In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.

Non-privileged accounts and roles are to be used for daily functions such as but not limited to email or internet browsing. This requirement limits exposure when operating from within privileged accounts or roles.

Security training, as directed by the Office of Information Security (OIS), must be completed by all privileged access users no less than annually or as deemed appropriate by OIS. Data Stewards are responsible for monitoring their own faculty, staff and students for compliance with the security training requirement and for and records retention related to security training.

Privileged access users shall take necessary precautions to protect the confidentiality and integrity of information encountered in the performance of their duties. If,

during the performance of their duties, users observe strange activity or evidence indicating misuse, they must immediately notify their supervisor and OIS at 558-4732 or abuse@uc.edu.

Definitions

Privileged Access: Access that allows an individual who can 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 or other such employees whose job duties require access to sensitive data residing on a system or network. This data can be paper or electronic data. For the purposes of this policy, application and other developers are also considered privileged.

Related links

Password Policy

Contact information

Office of Information Security	513-558-ISEC(4732)	infosec@uc.edu