University of CINCINNATI	*Policy Title:* **Privileged Access**	*Policy Number:* **9.1.14**
Category: Information Technology	**Effective Date:** 01/23/2019	**Policy Owner:** VP & CIO UC Information Technology
Policy applicable for: Faculty, Staff, Affiliates	**Prior Effective Date:** N/A	**Responsible Office(s):** IT@UC 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 user names and passwords that comply with the university 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.

The *Principle of Least Privilege* must be followed. Privileged Access users must have access set to the lowest level of access needed to accomplish their job function. Appropriate university leadership must approve all Privileged Access accounts and review all users with Privileged Access annually to determine if Privileged Access is still needed and to review what level of access is appropriate.

Privileged Access users should only have access on a *Need to Know* basis. The users should only have access to, and knowledge of, only 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.

Regular review of system logs is required to monitor Privileged Access user accounts for misuse. Appropriate logs must be maintained in a centralized system where integrity and access can be controlled. Logs must be sent to the university's Splunk implementation. If this is not possible then logs must be made available to the Office of Information Security for review when requested. The type of logs and the frequency of log review are to be determined based on the data classification and data types contained in the system. System owners must follow federal and state regulations and university policy in developing their log management and review procedures. For additional information please contact the Office of Information Security and/or reference NIST 800-92 Guide to Computer Security Log Management.

Privileged Access users' desktop or laptop computers must be university owned and must be managed by university controlled Endpoint Protection Services. When utilizing Privileged Access to access university systems, users must connect via the university's network. If access is required when off-campus, then the user must use the university's VPN and university approved multi-factor authentication. Wherever and whenever possible Privileged Access users must utilize university approved multi-factor authentication.

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. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices and operational guidelines pertaining to the activities of their local department.

Privileged Access use must be reserved for tasks that require the use of Privileged Access. If methods other than using Privileged Access will accomplish a task, those other methods must be used. If a Privileged Access user must submit data or access a system as an end-user, traditional means must be used to submit data or access a system (i.e. If a System Administrator must submit their annual benefit elections, they must do so as a normal user and not through Privileged Access not available to other users.) Every user of the system should operate using the least set of privileges necessary to complete the task. This principle limits the damage that can result from an accident or error.

It is important these individuals be familiar with relevant university policies and government regulations. IT@UC personnel with Privileged Access must review the detail of all university policies, specifically those related to information technology. The following polices must be reviewed, understood and implemented:

- Privileged Access Procedure
- Data Governance & Classification Policy
- Acceptable Use of University Information Technology Resources
- Password Policy
- Other Applicable Information Security Policies

Security training, as directed by the IT@UC 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. If any criminal activity is suspected, the user must also immediately contact the UC Police Department (UCPD) at 556-1111.

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

Acceptable Use of University Information Technology Resources
Data Governance & Classification Policy
NIST 800-92 Guide to Computer Security Log Management
Password Policy
Privileged Access Procedure
Other Applicable Information Security Policies

Contact information

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

History

Issued: 01/23/2019