Privileged Access Procedure

Background

The following procedure identifies required processes for lifecycle management of privileged access to University of Cincinnati (UC) information technology systems as defined by the Privileged Access Policy. Processes must be implemented to track requests for access, approvals, assignment, and removal of privileges. Regular review and audit of all privileged access must be performed no less than once per 12 months or more often for critical systems if required by the Data Trustee, Data Custodian, other university policy, or regulation.

Requesting Privileged Access

Data Trustees and Data Custodians must implement a process where any request for privileged access is documented and appropriately approved. This process must include the following steps:

1. Request for access is received and recorded in a consistent manner.
2. Request is verified and approved by the user's appropriate Dean/Vice President (or designee), Director, or Department Head.
3. Request is approved by the Data Trustee, Data Custodian, or Department of the application/system (as defined by the Data Trustee).
4. Access is provided to the user.
    a. In some cases, required training may be a prerequisite to access being granted.
5. All documentation must be available for audit.

Removing Privileged Access

Data Trustees and Data Custodians must implement a process where any request to remove privileged access is documented. Privileged access must be removed upon separation or change of job responsibilities within the university. This process must include the following steps:

1. Request for access removal is received and recorded in a consistent manner.
2. Request is initiated by the user, appropriate Dean/Vice President (or designee), Director, Data Trustee, Data Custodian, or Department of the application/system (as defined by the Data Trustee).
3. Access is removed from the user in a timely manner.
    a. Emergency access removal may be initiated by other entities (Human Resources, the Office of General Counsel, UC Public Safety, etc…) routed through the Office of Information Security.
4. All documentation must be available for audit.

Auditing Privileged Access

Data Trustees and Data Custodians must implement a process where all privileged access is reviewed and verified no less than once per 12 months or more often for critical systems if required by the Data Trustee, Data Custodian, other university policy, or regulation. This process must include the following steps:

1. Data Custodians will create a listing of all user accounts with privileged access on an application by application basis.
2. Data Custodians will communicate with the appropriate Dean/Vice President (or designee), Director, Data Trustee, Data Custodian, or Department of the application/system (as defined by the Data Trustee) to ensure that the level of privileged access is appropriate and necessary. A deadline for responding must be provided for the user to retain their access; otherwise access will automatically be removed.
3. Appropriate supervisors will validate that access is appropriate, necessary, and should be retained.
4. All inappropriate or unnecessary privileged access will be removed in a timely manner.
    a. Emergency access removal may be initiated by other entities (Human Resources, the Office of General Counsel, UC Public Safety, etc…) routed through the Office of Information Security.
5. A summary of audit activities must be provided to the Data Trustee, Data Custodian, or Department of the application/system (as defined by the Data Trustee) for approval.
6. All documentation must be available for audit.

ServiceNow

ServiceNow is the IT@UC recommended tool to be used to manage these workflows and retain necessary documentation for audit. Additional details on implementation of this workflow can be found in the ServiceNow Privileged Access Request Creation Process.

Related Links

Privileged Access Policy

Contact Information

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

History

Issued: 06/30/2020