INSERT COMPANY NAME AND LOGO HERE	
Title: IT User Access Revocation Policy	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy describes the different controls on information systems used to safeguard those data and systems during the user termination process.

Scope: This policy applies to all employees and other members of the workforce (whether paid, contractor or volunteer) working in all facilities under the organization's ownership.

Procedures:
The Human Resources Department (or other designated department), users, and their supervisors are required to notify network administration upon completion and/or termination of access needs and facilitate completion of the Termination Checklist.

The Human Resources Department, users, and supervisors are required to notify network administration to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and are filed with the Security Officer):

- The user has been using their access rights inappropriately
- A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password)
- An unauthorized individual is using a user's Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
- Network administration will terminate users' access rights immediately upon notification.
- The IT Department may audit and terminate access of users that have not logged into organization's information systems/applications for a period of over six (6) months.

Once notified of a workforce member's termination, IT is responsible for ensuring that:

- Password/credential access is immediately revoked in the event of an involuntary separation and scheduled to be revoked on the last day of employment for voluntary separations and at the end of temporary assignments for any workforce members.
- Access to all systems and applications is revoked immediately in the event of involuntary terminations and scheduled to be revoked on the last day of employment

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

for voluntary separations and at the end of temporary assignments for any workforce members.

- The workforce member is removed from any systems or applications that processed sensitive and regulated data immediately in the event of involuntary terminations and scheduled to be revoked on the last day of employment for voluntary separations and at the end of temporary assignments for any workforce member.

Human Resources and Supervisors/Department heads must coordinate to ensure that:

- Any keys and IDs provided to the workforce member during employment are returned on the scheduled last day of employment, or immediately upon notice of involuntary separation.
- In the event of an involuntary separation, the workforce member's supervisor and/or Human Resources will provide the workforce member limited and carefully supervised access to their desk or office.

Violations:

1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
2. Violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: Termination Checklist

Related Policies:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.