**Termination Policy**

**Purpose:**

It is the policy of [Insert Covered Entity or Business Associate name] to safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. As such, this policy describes the different termination requirements of the organization.

**Policy:**

1. Termination Procedures
   1. 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.
   2. The Human Resources Department, users, and supervisors are required to notify the 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 or Privacy Officer):
      1. The user has been using their access rights inappropriately
      2. 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)
      3. 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).
      4. Network administration will terminate users’ access rights immediately upon notification.
      5. 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.
   3. Once notified of a workforce member’s termination, IT is responsible for ensuring that:
      1. Password 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.
      2. 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 for voluntary separations and at the end of temporary assignments for any workforce members.
      3. The workforce member is removed from any systems or applications that processed ePHI 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.
2. Human Resources, Facilities, and supervisors must coordinate to ensure that:
   1. 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.
   2. 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 Covered Entity or Business Associate name] as determined by federal and state laws and regulations related to loss of data.