|  |  |  |
| --- | --- | --- |
| Policy #: | Title: | Effective Date: |
| x.xxx | Personnel Security Policy | MM/DD/YY |

PURPOSE  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

POLICY  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This policy is applicable to all departments and users of IT resources and assets.

1. POSITION RISK DESIGNATION

Information Technology (IT) shall:

* 1. Assign a risk designation to all positions.
  2. Establish screening criteria for individuals filling those positions.
  3. Review and update position risk designations [entity defined frequency].

1. PERSONNEL SCREENING

IT and department system and application owners shall:

* 1. Screen individuals prior to authorizing access to the information systems.
  2. Rescreen individuals according to [entity defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].
  3. Ensure personnel screening and rescreening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions.

1. PERSONNEL TERMINATION

Departments shall, upon termination of individual employment:

* 1. Disable information system access within [entity defined time period].
  2. Terminate/revoke any authenticators/credentials associated with the individual.
  3. Conduct exit interviews that include a discussion of [entity defined information security topics].
  4. Retrieve all security-related information system-related property.
  5. Retain access to information and information systems formerly controlled by terminated individual.
  6. Notify [entity defined personnel or roles] within [entity defined time period].

Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals.

The entity shall:

* 1. Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of information.
  2. Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the termination process as directed by Counsel and Human Resources (HR).
  3. Employ automated mechanisms to notify [entity defined personnel or roles] upon termination of an individual.

1. PERSONNEL TRANSFER

Departments shall:

1. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions.
2. Initiate [entity defined transfer or reassignment actions] within [entity defined time period following the formal transfer action].
3. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
4. Notify [entity defined personnel] within [entity defined time period] of transfer.

This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

1. ACCESS AGREEMENTS

Departments shall:

1. Develop and document access agreements for information systems.
2. Review and update the access agreements [entity defined frequency].
3. Ensure that individuals requiring access to information and information systems:
4. Sign appropriate access agreements prior to being granted access.
5. Re-sign access agreements to maintain access to information systems when access agreements have been updated or [entity defined frequency].

Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

1. THIRD-PARTY PERSONNEL SECURITY

IT Department shall:

* 1. Establish and document personnel security requirements including security roles and responsibilities for third-party providers.
  2. Require third-party providers to comply with personnel security policies and procedures established by the entity.
  3. Require third-party providers to notify [entity defined personnel] of any personnel transfers or terminations of third-party personnel who possess credentials and/or badges, or who have information system privileges within [entity defined time period].
  4. Monitor provider compliance.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

1. PERSONNEL SANCTIONS

IT and HR shall:

1. Employ a formal sanction process for individuals failing to comply with established information security policies and procedures
2. Notify [entity defined personnel] within [entity defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Sanction processes reflect applicable state and federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for those organizations.

COMPLIANCE

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |