Policy #:	Title:	Effective Date:
x.xxx	Access Control Policy	MM/DD/YY

PURPOSE

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164; NIST Federal Information Processing Standards (FIPS) 199

POLICY

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

1. ACCOUNT MANAGEMENT
   IT Department shall:

   a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

   b. Assign account managers for information system accounts.

   c. Establish conditions for group and role membership.

   d. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.

   e. Require approvals by system owners for requests to create information system accounts.

   f. Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

   g. Monitor the use of information system accounts.

h. Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.

i. Authorize access to the information system based on a valid access authorization or intended system usage.

j. Review accounts for compliance with account management requirements At least once every six months.

k. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

l. Employ automated mechanisms to support the management of information system accounts.

m. Ensure that the information system automatically disables temporary and emergency accounts after usage.

n. Ensure that the information system automatically disables inactive accounts after 90 days

o. Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

2. ACCESS ENFORCEMENT
   IT Department shall:

   a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

3. INFORMATION FLOW ENFORCEMENT
   IT Department shall:

   a. Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

4. SEPARATION OF DUTIES
   IT Department shall:
   a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

b. Document the separation of duties of individuals.

c. Define information system access authorizations to support separation of duties.

5. LEAST PRIVILEGE
   IT Department shall:

   a. Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

   b. Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

   c. Require that users of information system accounts, or roles, with access to sensitive assets, use non-privileged accounts or roles, when accessing non-security functions.

   d. Restrict privileged accounts on the information system , based on:
      i. Job classification and function.
      ii. Least privileges necessary to perform job responsibilities.

   e. Ensure that the information system audits the execution of privileged functions.

   f. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

6. UNSUCCESSFUL LOGON ATTEMPTS
   IT Department shall ensure that the information system:

   a. Enforces a limit of consecutive invalid logon attempts by a user during a five attempts.

   b. Locks the account/node automatically for 30 minutes or until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

7. SYSTEM USE NOTIFICATION
   IT Department shall ensure that the information system:

a. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

    i. Users are accessing a cisecurity information system.

    ii. Information system usage may be monitored, recorded, and subject to audit.

    iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.

    iv. Use of the information system indicates consent to monitoring and recording.

    v. There are not rights to privacy.

b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.

c. For publicly accessible systems, the IT Department shall ensure that the information system:

    i. Displays system use information, such as a warning banner or acceptable use notice, upon each user login session to systems within the cardholder data environment, before granting further access.

    ii. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

    iii. Includes a description of the authorized uses of the system.

8. SESSION LOCK
   IT Department shall ensure that the information system:

   a. Prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user.

   b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.

   c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

9. SESSION TERMINATION
   IT Department shall:

   a. Ensure that the information system automatically terminates a user session after 30 minutes.

10. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
    IT Department shall:

    a. Identify user actions that can be performed on the information system without identification or authentication consistent with organizational missions and business functions.

    b. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

11. REMOTE ACCESS
    IT Department shall:

    a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

    b. Authorize remote access to the information system prior to allowing such connections.

    c. Ensure that the information system monitors and controls remote access methods.

    d. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

        e. Ensure that the information system routes all remote accesses through a single, centrally managed network access control points to reduce the risk for external attacks.

    f. Authorize the execution of privileged commands and access to security-relevant information via remote access only for justified and approved use cases, such as emergency system maintenance or urgent security investigations, with strong authentication and activity monitoring in place.

    g. Document the rationale for such access in the security plan for the information system.

12. WIRELESS ACCESS
    IT Department shall:

    a. Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

    b. Authorize wireless access to the information system prior to allowing such connections.

    c. Ensure that the information system protects wireless access to the system using authentication of users and devices and encryption.

13. ACCESS CONTROL FOR MOBILE DEVICES
    IT Department shall:

    a. Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

    b. Authorize the connection of mobile devices to organizational information systems.

    c. Employ full-device encryption or container encryption to protect the confidentiality and integrity of information on approved devices.

14. USE OF EXTERNAL INFORMATION SYSTEMS
    IT Department shall:

    a. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

        i. Access the information system from external information systems.

        ii. Process, store, or transmit organization-controlled information using external information systems.

    b. Permit authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

        i. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan.

ii. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

15. INFORMATION SHARING
    IT Department shall:

    a. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for scenarios such as cross-department collaboration, incident response coordination, or joint vendor activities where user discretion is required..

    b. Employ automated mechanisms such as data classification tools, access control lists (ACLs), and collaboration platform security settings to assist users in making information sharing/collaboration decisions.

16. PUBLICLY ACCESSIBLE CONTENT
    IT Department shall:

    a. Designate individuals authorized to post information onto a publicly accessible information system.

    b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.

    c. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included.

    d. Review the content on the publicly accessible information system for nonpublic information based on a targeted risk analysis and removes such information, if discovered.

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