Revision History

Version	Date
Information Resource Access Control and Log Management Policy, 1.0	29 July 2021

INFORMATION RESOURCE ACCESS CONTROL AND LOG MANAGEMENT POLICY

I. Introduction

This Policy describes the process of authorizing, establishing, documenting, reviewing, and modifying appropriate access to USEIC Information Resources that process, transmit and/or store Organizational Data (as each term is defined in the USEIC Data Protection Charter (the "Charter")). Such access is limited to staff and contractors of the Organization who have been properly authorized to carry out legitimate business.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy

A. Requirements for System Owners and IT Custodians

Each System Owner and IT Custodian must ensure that the following access controls are implemented for any Information Resource:

1. Procedures for (a) establishing and describing different levels of User access, (b) authorizing User access and (c) granting, revising, and terminating User access are documented and periodically reviewed and revised as required so that access is granted only to Users who are necessary to accomplish the intended and approved purpose of the use.
2. The Information Resource is protected by authorization (access control) technology that employs unique User IDs and secret passwords unique to each User and password management procedures include the protections described in Section B below. Use of a generic group identifier is not recommended and is prohibited for access to a System that contains Sensitive Data.
3. Each Information Resource has a different administrative account and password and access to the password is restricted to as few people as possible. No unnecessary accounts are created on the Information Resource beyond those needed for administration and operation.
4. Access to the Information Resource locks after no more than 15 minutes of inactivity through an automatic locking mechanism, such as the use of a password protected screen saver or an equivalent alternative mechanism, unless the immediate area surrounding the Information Resource is physically secured or a waiver has been granted by the Data Protection Officer (DPO).
5. All unnecessary or unused accounts are disabled and removed.
6. User access to any System that uses, stores, or transmits Sensitive Data is reviewed on an annual basis.

B. Password Requirements

Each System Owner and IT Custodian must ensure that the following password protections are implemented for each Information Resource that processes, transmits or stores Sensitive Data:

1. Passwords are changed every 45-180 days.
2. Passwords may not be reused until two additional passwords have been used.
3. Users select and change their own passwords.
4. Passwords meet good password criteria, including:
   - Passwords must be at least 8 alpha and numeric characters long. Passwords for System Administrators or Service Accounts must be at least 16 characters long.
   - Dictionary words or commonly known proper nouns are not used unless the password has more than 12 characters.
   - Passwords include mixed case letters and numbers or special characters.
   - Users are encouraged to use a passphrase such as a sentence that contains the above requirements. In this case, dictionary words may be used.
5. Passwords are not displayed in clear text when being input into the System.
6. Default vendor or other pre-installed passwords are changed immediately following installation of a System.
7. The System "save password" feature is disabled.
8. Users are trained on good password practices.
9. If a password has been compromised, the user must enroll in MFA All to reinstate account access.

It is recommended, but not required, that the foregoing password procedures be implemented for Information Resources other than those that process, transmit or store Sensitive Data.

C. Log-In Requirements

Each System Owner and IT Custodian must ensure that the following log-in protections are implemented for each Information Resource:

1. System identifying information is minimized prior to successfully completing the log-in process.
2. The log-in process can (a) record failed log-in attempts and (b) upon completion of a successful log-in, record the date and time of the previous successful log-in.
3. Each System that processes, transmits, or stores Sensitive Data or Confidential Data has a login banner substantially in the form of the following text:

"The information in Systems at USEIC is private and confidential and may be used only on a need-to-know basis. All access is logged. Unauthorized or improper use of an Organization System or the data in it may result in termination and/or civil or criminal penalties."

D. Log Management

Each System Owner and IT Custodian must ensure that the following protections are implemented for each Information Resource that processes, transmits or stores Organizational Data:

1. Logging is activated on each Server.
2. Logging is configured to keep track of access to Systems and the Server itself.
3. Logs are retained for as long as it is operationally necessary; 29 days is recommended.
4. A Syslog or similar function is used to store logs on a separate System.
5. Logs are reviewed by the IT Custodian on a regular basis for unusual activity.
6. A process is established so that Log monitoring software is installed where available.
7. Logs generate the following information:
   - Date and time of activity;
   - Description of attempted or completed activity;

- Identification of User performing activity; and
- Origin of activity (i.e., IP address, workstation identifier, etc.)

8. Logs have audit mechanisms that generate reports of auditable events such as:
    - Failed authentication attempts;
    - Use of audit software programs or utilities (i.e., System logs);
    - Access to the System;
    - System start up or shut down;
    - Use of privileged accounts (i.e., System administrator accounts);
    - Security incidents;
    - Change of User's security information (i.e., User privileges); and
    - Vendor and temporary account activities.

E. Remote Access

Each User must ensure that the following controls are implemented to remotely connect to the Organization's Information Resources:

1. The controls meet or exceed the controls described in the USEIC Registration and Protection of Endpoints Policy.
2. The Organization's approved VPN is used, or the Information Resource is configured for remote access in a manner approved by the DPO.
3. The Organization's RDP (Remote Desktop Protocol) is either disabled by default or if RDP is enabled, the user must enrol in MFA to use a remote connection.