Procedure - Access Control

Purpose
The purpose of this procedure is to limit access to and prevent unauthorized access to information assets, which includes the responsibilities of provisioning and deprovisioning users and implementation of secure login procedures.

Access Controls and Need to Know
ESD will define and document access control rights and rules for each user or group of users based on position/role. Third party service providers shall be given clear statements of the business requirements met by these access controls. Access to information and information services will only be given on the basis of business and security requirements adhering to the following:

1. Access will be given on a need to know basis, based upon the security requirements and business requirements of individual business applications.
2. Access to information shall be provided in a manner that aims to protect the confidentiality and integrity of that information and without compromise to associated information or raw data.
3. Data owners shall review access control rights for users and groups of users on a periodic basis to ensure that all access rights are authorized and remain appropriate.
4. All forums where confidential information may be discussed and where non-ESD employees or agents are present shall be preceded by a determination that all parties are authorized to receive the information and the appropriate categorization of that information.
5. Access will be given that is consistent with security levels and classifications, consistent with state and federal policy and contractual obligations for confidentiality.
6. Access to standard common groups of users will be given standard access profiles (role-based security).
7. Access rights in a networked environment will recognize all connection types available.
8. Administrator access to production systems will be limited to only those with a justified business requirement for such access.

Types of Access Controls
ESD will establish clear access control rules that distinguish between optional, express, discretionary, automatic and those that require approval. Those access rules will adhere to the following:

1. Will specifically differentiate between those rules that are optional or conditional and those that are always to be enforced.
2. Will be declarative statements such as “access is forbidden unless specifically permitted” instead of “access is generally permitted unless forbidden”
3. Will differentiate between permissions that are granted by the information system and those permissions that must be granted by an administrator.

4. Will differentiate between those rules that require approval and those that do not. Access rules will consider changes in classifications that are automatic and those classification changes that must be initiated by an administrator.
5. For each system will be developed in according with the Information Classification guidelines commensurate with the information's sensitivity.

User Registration
A formal user registration and deregistration process will be used for gaining access to multi-user systems. This process must protect and maintain the security of access to the organization's information resources through the complete life cycle of the user and will adhere to the following:

1. Access to ESD confidential information shall be provided only after the authorization of the information owner has been obtained.
2. Contractors and third party contracts will contain the rights of access and will contain sanctions if unauthorized attempts at access are made.
3. Service providers shall be made aware of the procedure not to provide access to users until specific authorization has been given.
4. Each person accessing an ESD multi-user based information system shall utilize a unique ESD-assigned User ID and a private password. User IDs shall not be shared among two or more users.
5. System owners and/or management shall grant access rights. Formal records of all access rights for each system shall be maintained.
6. Access rights shall immediately be removed or modified when a user leaves the organization or changes jobs.

IT will periodically check for redundant IDs and ensuring that redundant IDs are not issued in excess of that required (i.e., administrators may have a privileged and a non-privileged account on the same system, but an average user should not have two different non-privileged accounts on the same system without a valid business reason).

Privilege Management
User rights shall be granted using the least-privilege methodology, based on business need and security requirements.

All privileges shall be granted only with formal authorization. This authorization shall be accomplished along with User ID authorization, according to IT guidelines. All privileges that are granted will be documented. No privileges shall be granted until authorization is complete.

Elevated privileges (Administrator or root, etc.) should be assigned to a different user ID than that used for normal business use. Administrators should only use their elevated privilege accounts when conducting activities that actually require them. Elevated privileges must only be assigned to dedicated systems administrators and not normal users.

Wherever possible system routines should be developed and used instead of privileges.

Review of User Access Rights
Users' access rights will be reviewed at regular intervals. Managers will review their employee's rights to ensure they are consistent with their present job function. IT will review user rights to ensure that elevated privileges have not been granted out without authorization, and that

accounts that have not been used recently or belong to terminated employees are deactivated or purged.

Password Use
Users will be granted initial temporary passwords and will be forced to change them immediately. Initial passwords will be unique for each user. Temporary passwords will only be granted with positive identification of the user. Passwords will be given in a secure manner.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of ESD's entire corporate network. As such, all ESD employees (including contractors and vendors with access to ESD systems) are responsible for taking the appropriate steps to select and secure their passwords as defined by IT.

The scope of this procedure includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ESD facility, has access to the ESD network, or stores any non-public ESD information.

Use of Network Services
Users shall only have access where there is a specific business requirement and the access has been specifically authorized. Users will be granted specific access to networks that they are permitted to access. Users may not access networks that they are not given specific authorization to access.

Third parties that must deploy non-ESD controlled systems must be specifically approved by the Designated Information Security Officer. Network Controls must segregate groups of information services, users and information systems when interconnecting networks to partners or other third parties.

Acceptable Use of ESD Computer Systems
Board Policy 2022: Electronic Resources and Internet Safety is the ESD's acceptable use policy for use of information systems. All employees acknowledge the policy before network and email credentials are issued.

Access to Network and Network Services
The principle of least access will be applied as the general approach for protection of information assets. Changes to this approach require documented approval from both the Data Owner and Designated Information Security Officer.

Timeline for Implementation of Procedure
Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure's periodic review. If an operating practice is needed from IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.