Procedure - Physical and Environmental Security

Purpose
The purpose of this procedure is to protect ESD’s physical premises and the equipment in which information assets are stored.

Physical Security Controls
Physical entry controls will be used to protect all secure areas. These controls will be designed to prevent unauthorized access, damage or interference to the business that take place within the area. Physical security controls apply to any ESD owned or controlled facility, including temporary locations.

Site Risk Assessment
A risk assessment of secure areas to determine the type and strength of the physical entry control that is appropriate and prudent. The security controls for an area should be commensurate with the value and classification of the information resources contained therein. This risk assessment must also take into account the physical surroundings of the site. Finally, physical security requirements should include items such as plumbing and electrical wiring as these may not always be mandated by local authorities.

Site risk assessments must be conducted for any sites where ESD will be sharing facilities with any outside organization. This may be sharing a building (where physical access is common to all, but network access is specific to each organization) or where ESD is sharing a suite (where physical and network access is common to all) with others. Specific security requirements must be determined for these situations, based on the arrangements.

Where sites are deficient in physical security controls (such as leased sites where the owner will not allow modification to the structure, or shared sites with business partners), additional network security controls are warranted to protect the rest of the corporate network. In addition, the levels of sensitivity of information that can be processed or stored there may be restricted.

Restricted Access to Sites
Access to sensitive information and information processing facilities will be restricted to authorized persons only. Authentication controls will be used to authorize and validate entry. Physical barriers (i.e., doors) must be of sufficient strength and construction to deter entry, based on the results of the risk assessment.

Controls to restrict access to facilities will be determined on a case-by-case basis. These controls will ensure that unauthorized persons do not have easy physical access to the facilities, and such access is detected, and the appropriate personnel notified if a breach occurs. The Information Security Officer will develop, implement, and review operating practices for access controls and other physical security measurements commensurate with the classification levels of data present and the information protection requirements.

Access rights will be given on a least-privilege basis and will be as granular as necessary to appropriately protect various classifications of information or facilities. Access rights to secure areas will be reviewed by the site manager periodically and updated where necessary.

Visitor Procedures
All visitors to sensitive areas (i.e., anywhere handling confidential data) will only be allowed for authorized purposes. Those visitors shall attach a visitor's badge to their person or shall always be escorted by an employee with authorized access to that area. A visitors' log will be in place at all secure areas that record the date and time of entry and exit times. All visitors will be given both security instructions and emergency procedures (if applicable).

Employees will challenge unfamiliar people who are unescorted or not showing visible identification.

Contractors, service vendors, suppliers, material men, etc., shall be advised of the building rules and regulations concerning their proper conduct within ESD's property.

Third Party Physical Security at ESD Facilities
Special situations may arise where third parties will have personnel and devices at ESD facilities on a full-time basis. These third parties must only be allowed full-time access if they serve to augment the core capability or flow of ESD's business. Special care should be taken to limit access of third-party personnel to only their work areas as much as possible.

Control of Physical Security Controls
Access to the mechanisms that control physical access to secure sites must be done on the least-privilege basis. This includes access to badge enabling systems, door lock keys, or any other physical access control systems. Master badges or keys must be restricted to very few individuals per site or system. Wherever possible, control of these systems must reside with the local Information Security or Physical Security management.

Securing Offices, Rooms, and Facilities
All offices, rooms and facilities that contain resources other than public information will be protected accordingly to prevent unauthorized access, damage or interference to business processes.

Securing Sites when Unoccupied
Rooms in facilities that contain sensitive assets will be locked when not in use. Windows and doors will be kept locked and have protection from intrusion or environmental factors. Intrusion alarms will be in place and maintained to the vendors' standards as applicable according to the information protection requirements. Unoccupied areas will be alarmed as required.

Sensitive documents will be locked in file cabinets or other protective furniture that take into account the results of the risk analysis.

Additional controls will be implemented for computer and communications rooms or areas. Key facilities will be situated so as to avoid public access. Support functions and equipment will be situated in a way that keeps them away from the public and unauthorized personnel.

Signage and Directory Listings for Secure Sites
The uses of buildings that contain information assets or processing facilities will be unobtrusive and not marked in such a way that gives the public an indication of their purpose or function.

Directories and telephone books that provide information on locations of sensitive facilities shall be secured from unauthorized access.

Monitoring of Facilities for Physical Security
Where possible, systems shall monitor the physical security of facilities. Monitoring could include any or all of the following technologies, based on the outcome of the physical security risk assessment:

- Closed circuit TV or video cameras
- Glass break sensors
- Door and window opening alarms
- Hold open sensors for doors or windows
- Always-active door alarms for emergency exits and other little used doors
- Above or below ceiling sensors (sites with false ceilings and walls that do not extend from floor to ceiling
- Motion/heat sensors for sensitive working areas
- Security patrols

Other Site Security Issues
Hazardous or combustible materials shall be stored securely a safe distance from secure facilities. Only necessary bulk supplies shall be stored within secure facilities.

Back-up equipment and media shall be stored off-site and a safe distance from facilities sufficient that it would not be damaged if the facility is damaged.

Removal of Assets
ESD mobile devices are intended to be used offsite to support the itinerant nature of the business requirements. The information assets are protected as mobile devices and returned as part of the return of assets.

Secure Disposal of Equipment
ESD shall follow NIST Special Publication 800-88 Revision 1 or subsequent publications for secure disposal of equipment. Exceptions to this shall be approved by the Information Security Officer.

Unattended User Equipment
Users shall protect ESD's information resources from unauthorized access by protecting unattended equipment:

- Users will terminate active sessions when finished (or unattended) or secure by appropriate locking functions.
- Users will log off of multi-user systems when finished.
- Users will log off or lock terminals when unattended.
- PCs or terminals shall be locked (i.e. by a key or password) when not in use.
- A password-protected screen saver will be automatically invoked after 15 minutes of inactivity.

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.