Information Technology Branch Physical and Environmental Security Technical Standard

Information Management,
Administrative Directive A1461

Cyber Security Technical Standard # 3

November 20, 2014

Approved: **Date**: November 20, 2014

1. Purpose

This technical standard identifies the requirements to identify and manage physical and environmental threats against Information Technology Branch technology systems and the premises where those systems reside. This is achieved by establishing minimum controls for the physical security of technology systems.

2. Scope

This technical standard is intended to apply to people, equipment, application systems and processes that fall within the direct organizational control and support responsibilities of the Information Technology Branch of Corporate Services Department.

3. Exceptions and Compensating Controls

In cases where business requirements or technology limitations prevent direct compliance with an implementation expectation, compensating controls can be proposed that meet the statement objective. If an interpretation is required, contact the Program Manager, IT Security and Risk Assurance Program, Information Technology Branch for guidance. Special cases where exceptions are required to meet business requirements or technology limitations need to be documented and approved.

4. Technical Standards and Implementation Expectations

Implementation expectations establish baseline behaviors and actions that are consistent with industry standards or best practices to meet the technical standard statements. It is the intention of this section to establish baseline security requirements in support of business operations, not to impede business operations or define specific technologies or methodologies.

The technical standards do not provide exacting and prescriptive guidance on exactly how to perform everything stated within the standard. In most cases, additional specific how-to procedures will need to be developed.

4.1. Secure Areas Technical Standard

4.1.1. *IT Branch data processing facilities must be protected by a physical security perimeter*.

4.1.1.1. Implementation Expectations

IT Branch should ensure appropriate controls are applied to secure areas that provide for employee safety and for the protection of information and technology assets.

Appropriate security controls should be evaluated to reduce the level of identified risks. These can include:

- Where possible, walls surrounding the facility are to be extended from

true floor to true ceiling (slab to slab), to prevent unauthorized entry. Appropriate control mechanisms (e.g., locks, alarms and bars on windows and doors) may be applied;
- IT Branch data processing facilities may be equipped with doors that close automatically; and,
- Access to secure areas may be controlled, authorized and monitored by appropriate methods.

Physical security and environmental controls pertaining to IT Branch data processing facilities should be tested and reviewed regularly.

4.1.2. *IT Branch data processing facilities must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access*.

4.1.2.1. Implementation Expectations

Appropriate entry controls should be considered for physically accessing IT Branch data processing facilities. These can include:
- Recording the date and time of entry and departure of visitors;
- Visitors are to be supervised unless unsupervised access has been approved;
- Visitors are to only be granted access for specific, authorized purposes;
- Employees and visitors are required to wear some form of visible identification;
- Employees can be granted restricted access to secure areas only when required and access must be authorized and monitored; and
- Access rights to secure areas are to be regularly reviewed and updated, and revoked when necessary.

Entry controls pertaining to IT Branch data processing facilities should be tested and reviewed regularly.

4.2. Equipment Security Technical Standard

4.2.1. IT Branch equipment must be protected to reduce the risks from unauthorized access, environmental threats and hazards.

4.2.1.1. Implementation Expectations

The following items are recommended for consideration to protect equipment:
- Equipment is to be located to minimize unnecessary access into work areas;
- Items requiring special protection are to be isolated to increase the level of protection provided;
- Controls are to be adopted to minimize the risk of potential physical threats, (e.g. theft, fire, explosives, water or water supply failure, vibration, electrical supply interference, and vandalism); and
- Environmental conditions, such as temperature and humidity are to be monitored for conditions which could adversely affect the operation of computing equipment in data processing facilities.

4.2.2. IT Branch data processing equipment must be protected from power supply interruption and other disruptions caused by failures in supporting utilities.

4.2.2.1. Implementation Expectations

The following items are recommended for consideration to protect equipment in IT Branch data processing facilities from disruptions in supporting utilities:

- Uninterruptible power supply, back-up generators, and fuel, as required by business and technical requirements;
- Emergency power off switches located near emergency exits in equipment rooms;
- Emergency lighting;
- Alarms to indicate inadequate water pressure for fire suppression;
- Alarms to indicate malfunctions in heating, ventilation, air conditioning, humidity control and sewage systems; and
- Multiple connections to the power utility for critical systems and equipment.

4.2.3. IT Branch equipment must be correctly maintained to enable continued confidentiality, availability and integrity.

4.2.3.1. Implementation Expectations

IT Branch equipment being repaired or undergoing maintenance should be done in accordance to the supplier's specifications. The following items are recommended for consideration to protect equipment:

- Ensuring the scheduling of routine preventive maintenance of equipment by qualified authorized personnel;
- Ensuring that maintenance is performed in accordance with the manufacturer's specifications, in compliance with warranty requirements, and using safe practices;
- Ensuring that, where possible, maintenance is scheduled during approved change windows to avoid interference with services or operations;
- Notifying affected users prior to taking equipment off-line for scheduled maintenance;
- Maintaining records to identify trends, weaknesses and additional maintenance requirements.

5. Reference

Further information can be found in:

- ISO 27002, Chapter 9 – Physical and Environmental Security