HPOL#05
Physical and Environmental Security

(Version 1.0)

Table of Contents

5.1. SCOPE AND OBJECTIVES

Government organizations shall provide physically and environmentally secure environments to house and protect systems, information, and people from hostile external influences through the provision of multiple physical and environmental security perimeters.

Information is protected only when all potential avenues for access or disruption are addressed. In addition to logical security threats, information can be highly susceptible to physical threats such as theft, physical damage, flood, fire, temperature fluctuations and other environmental changes. For these reasons, a physical and environmentally controlled situation must exist to complement the logical protection.

This policy establishes guidelines to prevent unauthorized access and interference to government organization premises and information assets. It also suggests guidelines to build security controls to prevent damage from physical security threats and environmental hazards.

5.2. POLICY STATEMENT

5.2.1. FACILITY CONTROL AND SECURE AREAS

5.2.1.1. Physical Security Perimeters

5.2.1.1.1. The physical security perimeters will be clearly defined by the government organization based on risk assessments for the area and its contents.

Explanatory Notes

Considerations include but are not be limited to:

Physical areas will be established with various perimeter vehicles such as walls, attended screening areas, offices and secured rooms, lockable cabinets, safes and fire safes.

The government organization building perimeter, office perimeter and perimeters for internally restricted areas will be of physically sound construction with strongly constructed continuous floor to ceiling walls and appropriately sound and secured entryways.

Any secondary, unattended, access points will be subject to strong control from physical and personnel measures.

Perimeters will be designed to address environmental protection (e.g., fire and flood) as well as physical access.

When the site is unattended, physical perimeters will be monitored by controls such as security guards, burglar alarms, or Closed Circuit Television.

5.2.1.2. General Access

5.2.1.2.1. The government organization will restrict access to sites and buildings and internally confidential or restricted areas to authorized personnel only and visitors will be subject to additional controls.

5.2.1.2.2. Site access outside of regular office hours will be granted only to authorized individuals.

5.2.1.2.3. A continuously controlled reception area will appropriately restrict access to the rest of the premises during business hours.

5.2.1.3. Visitor Access Controls

5.2.1.3.1. Visitors will be required to fill a visitor log.

Explanatory Notes

The log would include but not be limited to the record of date, time in, time out, person visited at the government organization, and reason for the visit.

5.2.1.3.2. Visitors to the general government organization offices will be met by their government organization contact at the reception and will be escorted at all times through the government organization offices.

5.2.1.3.3. Individuals contracted to perform work at the government organization offices will be allowed to operate with reduced supervision, however, these visitors must still comply with other visitor access controls.

5.2.1.3.4. The visitor sponsor will assume responsibility for that visitor for the duration of their stay.

Explanatory Notes

The visitor sponsor will ensure that visitors are appropriately logged including immediate completion of the visitor sign-out process if departure occurs through an access point other than the reception.

5.2.1.3.5. Personnel and visitors must log their belongings before entering restricted premises.

Explanatory Notes

Examples of belongings to be declared are laptop computer, mobile phones etc. The security guard must verify the declarations to prevent removal of government organization property from the premises.

5.2.1.3.6. Visitors will be granted access to Confidential or Restricted areas only with authorization and continuous supervision.

5.2.1.3.7. All unescorted visitors will be instructed on applicable government organization physical and personnel security requirements.

5.2.1.3.8. All former employees will be treated as visitors for the purposes of access to the government organization facilities and will not be granted any special dispensations.

5.2.1.3.9. Any visitors without a displayed badge will be escorted back to the reception area for identification and authorization of access.

5.2.1.4. Securing Offices, Rooms, and Facilities

5.2.1.4.1. Established areas will be protected appropriately, in accordance with risk assessments for that area.

<u>Explanatory Notes</u>

Protection is required, for example, from damage caused by environmental factors such as fire, flood, explosion, other natural or person-made disaster, and power, temperature and humidity variations, in addition to protection from unauthorized physical access.

5.2.1.4.2. Consideration will be given to potential for threats posed by adjacent or neighbouring premises.

5.2.1.4.3. Confidential and restricted areas will be sited to avoid access by the general public and will be unobtrusive so as to give no obvious signs as to the purpose of the area.

5.2.1.4.4. Support functions and equipment (e.g., printers, faxes) for confidential and restricted areas will be sited within the area, wherever appropriate.

5.2.1.4.5. Confidential and restricted areas will be secured when unattended.

5.2.1.4.6. Restricted areas will be periodically checked when unattended to prevent and detect unauthorized access.

5.2.1.4.7. Hazardous and combustible materials will be safely stored outside of restricted areas at a safe distance.

5.2.1.5. Inspection of Incoming and Outgoing Packages

5.2.1.5.1. Inspection of incoming and outgoing packages must be conducted.

Explanatory Notes

Examples of packages would be bags, briefcases, boxes, laptop computers, etc. Inspection must be conducted to ensure that unauthorized materials are not brought in or taken out of the government organization premises. All incoming material should be declared at the security office and a gate pass document obtained for clearance of the same. Any material / article belonging to the government organization, taken out of the premises, should be supported by a gate pass duly approved by personnel designated by management.

5.2.1.6. Sensitive and Restricted Area Access

5.2.1.6.1. Access to sensitive and restricted areas will be restricted to authorized personnel on a “need to access” basis only.

Explanatory Notes

General government organization staff will not have access to these areas.

5.2.1.6.2. Sensitive and restricted areas will be subject to additional entry controls such as locks, registers or swipe cards.

5.2.1.6.3. An audit trail of access to sensitive and restricted areas will be maintained and periodically reviewed.

5.2.1.6.4. Access privileges to sensitive and restricted areas will be reviewed regularly.

Explanatory Notes

This would be performed in order to assess accuracy of the contained information.

5.2.1.6.5. Personnel will be informed of the activities within sensitive and restricted areas on a "need to know" basis only.

5.2.1.6.6. No combustible or hazardous materials should be allowed in restricted zones demarcated for the purpose.

5.2.1.6.7. External photographic or video equipment will not be allowed within sensitive or restricted areas.

5.2.1.7. Identification

5.2.1.7.1. All government organization employees will be required to prominently display staff identification cards.

Explanatory Notes

This would be to allow easy identification for authorized access. Wherever possible, picture ID cards will be employed to prevent badge sharing and to strongly identify authorized individuals.

5.2.1.7.2. Government organization employees will be required to sign in at the reception and will obtain and display a visitor badge where staff IDs have been forgotten.

5.2.1.7.3. All visitors will be required to prominently display visitor badges.

Explanatory Notes

The visitor badges should be of different colour or configuration so that they could be identified quickly and conveniently.

5.2.1.8. Revocation of Access Privileges

5.2.1.8.1. Identification cards, access cards, keys, and other vehicles for access will be collected and deactivated upon separation or termination of staff.

5.2.1.8.2. Relevant individuals will be informed of staff departures.

Explanatory Notes

At a minimum, key individuals such as managers, reception, and immediate co-workers should be informed to facilitate identification of subsequent unauthorized access by the separated or terminated individual.

5.2.1.9. Delivery and Loading Areas

5.2.1.9.1. Delivery and loading areas will be segregated from the rest of the government organization operations.

Explanatory Notes

Segregation is required particularly from sensitive and restricted areas to control deliveries and to minimize access to the operating facilities for these purposes.

5.2.1.9.2. Items entering and leaving the premises of the government organization must be inspected and registered.

Explanatory Notes

Items would include but not be limited to materials, supplies and equipment. Inspection and registration shall be in accordance with the government organization's standard procedures for material handling.

5.2.1.10. Safety Measures within the Premises

5.2.1.10.1. The premises of the government organization must be appropriately constructed. Fire-proof safes should be made use of for data protection.

Explanatory Notes

Construction should be with fire resistant materials and it should be structurally stable to withstand fire or environmental damage.

5.2.1.10.2. Smoking should be banned in the premises of the government organization as per Public Administration Circular No: 08/99 on “Prohibition of Smoking in State Institutions”.

5.2.1.10.3. No consumption of food and beverage should be permitted in areas housing equipment and/or other media.

5.2.1.10.4. Proper training should be given to all staff members on the use of safety measures.

5.2.1.10.5. The government organization should ensure the availability of documented and tested emergency evacuation plans.

5.2.2. EQUIPMENT AND OTHER MEDIA SECURITY

5.2.2.1. Equipment Siting and Protection

5.2.2.1.1. All equipment will be sited within the government organization facilities in a way commensurate with the risk assessment for that equipment and the information that it handles.

Explanatory Notes

The objective would be that unnecessary and unauthorized access potential is minimized.

5.2.2.1.2. Sensitive equipment will be positioned to prevent viewing by other potentially unauthorized staff during use.

5.2.2.1.3. Threats to the government organization will be identified, and controls appropriate for risk assessments will be implemented.

Explanatory Notes

The objective would be to reduce the potential for incident.

5.2.2.1.4. All equipment should be insured.

Explanatory Notes

All equipment should have adequate insurance based on the value of the equipment.

5.2.2.1.5. Environmental conditions will be monitored in appropriate areas.

Explanatory Notes

At a minimum, monitoring will be performed for fire / smoke in the general facility areas. Further, sensitive or restricted areas will be subject to additional monitoring for temperature, water, power continuity / cleanliness, and humidity.

5.2.2.1.6. Environmental controls will be implemented in facilities in accordance with risk assessments.

Explanatory Notes

Environmental controls will include but not be limited to heating, ventilation, air conditioning, drainage, fire suppression, emergency lighting, continuous power and humidity control. Computer rooms will contain elements of each environmental control at sufficient levels.

5.2.2.2. Power Supplies

5.2.2.2.1. Continuous power will be provided for sensitive assets.

Explanatory Notes

Continuous power will be provided through, at a minimum, Uninterruptible Power Supply (UPS) protection. Consideration for generator backup may be contemplated if risk assessments warrant. Fallback plans must describe in detail the action to be taken in case of a continued power outage.

5.2.2.2.2. Power supplies will be subject to controls that will ensure 'clean' power to sensitive equipment.

5.2.2.2.3. Electrical supply must conform to the manufacturer's specifications for each piece of equipment.

5.2.2.2.4. Clearly defined controls and procedures to effect orderly shutdown of computing resources in the event of a prolonged power failure will be documented and communicated to all individuals responsible for computing resources.

5.2.2.2.5. The government organization will ensure the installation of emergency power off switches in strategic locations.

<u>Explanatory Notes</u>

Emergency power off switches would have adequate labeling, and be shielded to avoid accidental activation.

5.2.2.3. Network and Cabling Security

5.2.2.3.1. Power and telecommunications cabling will be appropriately protected at all termination points (e.g., entry / exit points to facility).

5.2.2.3.2. Network cabling will be routed or protected to prevent unauthorized access that could result in disruption of service or interception of information.

5.2.2.3.3. Power and network cabling will be routed to prevent electrical interference with network traffic.

5.2.2.4. Equipment Maintenance

5.2.2.4.1. Equipment must be maintained in accordance with government organization procedures, standards and guidelines for equipment maintenance.

<u>Explanatory Notes</u>

As a minimum, these standards will recognize the criticality of the equipment and will comply with the vendor's recommendations and specifications.

5.2.2.4.2. Maintenance of government organization equipment must be performed only by authorized and qualified maintenance personnel.

5.2.2.4.3. Equipment maintenance will be performed on-site whenever possible.

Explanatory Notes

If offsite maintenance or repair is required, the government organization will take appropriate measures to protect the confidentiality and integrity of the information that may be stored on that asset.

5.2.2.4.4. Maintenance will be tracked and logged for each asset.

5.2.2.5. Security of Equipment Off-Premises

5.2.2.5.1. Equipment will only be allowed offsite for valid reasons with written authorization by management of the government organization.

5.2.2.5.2. Individuals taking equipment offsite will provide protection commensurate with that provided at the government organization offices.

5.2.2.5.3. Equipment taken offsite will not be left unattended in public areas and will only be left unattended in specified locations such as the employee's place of residence.

Explanatory Notes

Employees will retain personal control over the assets at all times until the specified location is reached.

5.2.2.5.4. Portable computing assets are not used to fulfil government organization purposes in public areas unless unauthorized viewing of activity on-screen can reasonably be prevented.

5.2.2.6. Secure Disposal or Re-use of Equipment and Other Media

5.2.2.6.1. Media is disposed of when no longer required.

Explanatory Notes

To reduce the risk of accidental disclosure of sensitive information, the information owner ensures that a secure disposal (e.g., incineration, shredding, or purging) is performed for media containing internal or confidential information.

5.2.2.6.2. The government organization will re-use, sell, or donate upgraded or decommissioned assets only if doing so does not jeopardize sensitive or potentially damaging organizational information.

5.2.2.6.3. Storage media on which confidential information was stored will have information removed and/or will be overwritten prior to sale or donation.

Explanatory Notes

The objective of overwriting prior to sale or donation is to prevent information access and to mitigate software licence breaches.

5.2.2.6.4. If the storage media is to be disposed of, it will be physically destroyed prior to doing so.

5.2.2.6.5. The disposal of media containing confidential information is logged to maintain an audit trail, as appropriate.

5.2.2.7. Management of Removable Media

5.2.2.7.1. All removable media will be re-used or disposed of in a manner commensurate with non-removable media criteria.

5.2.2.7.2. Authorization from the information owner is required for all media removed from the government organization and a documented log is maintained, where appropriate.

5.2.2.7.3. The information owner will ensure that all media is stored in a physically secure environment, and in accordance with manufacturers' specifications.

5.2.2.7.4. Confidential shredding bins and removable media disposition bins will be provided in designated areas of the premises to facilitate secure disposal.

5.2.2.7.5. Removable media deposited in provided bins will be physically destroyed prior to disposal.

5.2.2.8. Security of System Documentation

5.2.2.8.1. Confidential documentation is securely stored, either physically or electronically, and its access is granted only with authorization from the owner.

Explanatory Notes

Confidential documentation would include but not be limited to applications, systems, and business processes.

5.2.2.9. Clear Desk and Clear Screen Policy

5.2.2.9.1. Computers and terminals will not be left logged on when unattended and will be protected by locking or shutting down when unattended.

5.2.2.9.2. Computers and terminals will be shut down when not in use.

5.2.2.9.3. Sensitive information on paper or removable media must be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.

5.2.2.9.4. Faxes and photocopiers will be sited to protect against unauthorized access and will be cleared of unclaimed content at pre-determined intervals.

5.2.2.9.5. When printing or copying sensitive information, it is the responsibility of the initiator to ensure the copies or printouts are cleared from the machine immediately.