Purpose

To prevent or reduce the consequences of events originating from physical and environmental threats.

Guidance

Risk assessments to identify the potential consequences of physical and environmental threats should be performed prior to beginning critical operations at a physical site, and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

Physical premises location and construction should take account of:

a) local topography, such as appropriate elevation, bodies of water and tectonic fault lines;

b) urban threats, such as locations with a high profile for attracting political unrest, criminal activity or terrorist attacks.

Based on risk assessment results, relevant physical and environmental threats should be identified and appropriate controls considered in the following contexts as examples:

a) fire: installing and configuring systems able to detect fires at an early stage to send alarms or trigger fire suppression systems in order to prevent fire damage to storage media and to related information processing systems. Fire suppression should be performed using the most appropriate substance with regard to the surrounding environment (e.g. gas in confined spaces);

b) flooding: installing systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems. Water pumps or equivalent means should be readily made available in case flooding occurs;

c) electrical surges: adopting systems able to protect both server and client information systems against electrical surges or similar events to minimize the consequences of such events;

d) explosives and weapons: performing random inspections for the presence of explosives or weapons on personnel, vehicles or goods entering sensitive information processing facilities.

Other information

Safes or other forms of secure storage facilities can protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Organizations can consider the concepts of crime prevention through environmental design when designing the controls to secure their environment and reduce urban threats. For example, instead of using bollards, statues or water features can serve as both a feature and a physical barrier.

7.6 Working in secure areas

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control

Security measures for working in secure areas should be designed and implemented.

Purpose

To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

Guidance

The security measures for working in secure areas should apply to all personnel and cover all activities taking place in the secure area.

The following guidelines should be considered:

a) making personnel aware only of the existence of, or activities within, a secure area on a need-to-know basis;

b) avoiding unsupervised work in secure areas both for safety reasons and to reduce chances for malicious activities;

c) physically locking and periodically inspecting vacant secure areas;

d) not allowing photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized;

e) appropriately controlling the carrying and use of user endpoint devices in secure areas;

f) posting emergency procedures in a readily visible or accessible manner.

Other information

No other information.

7.7 Clear desk and clear screen

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

Control

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Purpose

To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

Guidance

The organization should establish and communicate a topic-specific policy on clear desk and clear screen to all relevant interested parties.

The following guidelines should be considered:

a) locking away sensitive or critical business information (e.g. on paper or on electronic storage media) (ideally in a safe, cabinet or other form of security furniture) when not required, especially when the office is vacated;

b) protecting user endpoint devices by key locks or other security means when not in use or unattended;

c) leaving user endpoint devices logged off or protected with a screen and keyboard locking mechanism controlled by a user authentication mechanism when unattended. All computers and systems should be configured with a timeout or automatic logout feature;

d) making the originator collect outputs from printers or multi-function devices immediately. The use of printers with an authentication function, so the originators are the only ones who can get their printouts and only when standing next to the printer;

e) securely storing documents and removable storage media containing sensitive information and, when no longer required, discarding them using secure disposal mechanisms;

f) establishing and communicating rules and guidance for the configuration of pop-ups on screens (e.g. turning off the new email and messaging pop-ups, if possible, during presentations, screen sharing or in a public area);

g) clearing sensitive or critical information on whiteboards and other types of display when no longer required.

The organization should have procedures in place when vacating facilities including conducting a final sweep prior to leaving to ensure the organization's assets are not left behind (e.g. documents fallen behind drawers or furniture).

Other information

No other information.

7.8 Equipment siting and protection

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Equipment should be sited securely and protected.

Purpose

To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

Guidance

The following guidelines should be considered to protect equipment:

a) siting equipment to minimize unnecessary access into work areas and to avoid unauthorized access;

b) carefully positioning information processing facilities handling sensitive data to reduce the risk of information being viewed by unauthorized persons during their use;

c) adopting controls to minimize the risk of potential physical and environmental threats [e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism];

d) establishing guidelines for eating, drinking and smoking in proximity to information processing facilities;

e) monitoring environmental conditions, such as temperature and humidity, for conditions which can adversely affect the operation of information processing facilities;

f) applying lightning protection to all buildings and fitting lightning protection filters to all incoming power and communications lines;

g) considering the use of special protection methods, such as keyboard membranes, for equipment in industrial environments;

h) protecting equipment processing confidential information to minimize the risk of information leakage due to electromagnetic emanation;

i) physically separating information processing facilities managed by the organization from those not managed by the organization.

Other information

No other information.

7.9 Security of assets off-premises

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Off-site assets should be protected.

Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

Guidance

Any device used outside the organization's premises which stores or processes information (e.g. mobile device), including devices owned by the organization and devices owned privately and used on behalf of the organization [bring your own device (BYOD)] needs protection. The use of these devices should be authorized by management.

The following guidelines should be considered for the protection of devices which store or process information outside the organization's premises:

a) not leaving equipment and storage media taken off premises unattended in public and unsecured places;

b) observing manufacturers' instructions for protecting equipment at all times (e.g. protection against exposure to strong electromagnetic fields, water, heat, humidity, dust);

c) when off-premises equipment is transferred among different individuals or interested parties, maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment. Information that does not need to be transferred with the asset should be securely deleted before the transfer;

d) where necessary and practical, requiring authorization for equipment and media to be removed from the organization's premises and keeping a record of such removals in order to maintain an audit trail (see 5.14);

e) protecting against viewing information on a device (e.g. mobile or laptop) on public transport, and the risks associated with shoulder surfing;

f) implementing location tracking and ability for remote wiping of devices.

Permanent installation of equipment outside the organization's premises [such as antennas and automated teller machines (ATMs)] can be subject to higher risk of damage, theft or eavesdropping. These risks can vary considerably between locations and should be taken into account in determining the most appropriate measures. The following guidelines should be considered when siting this equipment outside of the organization's premises:

a) physical security monitoring (see 7.4);

b) protecting against physical and environmental threats (see 7.5);

c) physical access and tamper proofing controls;

d) logical access controls.

Other information

More information about other aspects of protecting information storing and processing equipment and user endpoint devices can be found in 8.1 and 6.7.

7.10 Storage media

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control

Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Purpose

To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

Guidance

Removable storage media

The following guidelines for the management of removable storage media should be considered:

a) establishing a topic-specific policy on the management of removable storage media and communicating such topic- specific policy to anyone who uses or handles removable storage media;

b) where necessary and practical, requiring authorization for storage media to be removed from the organization and keeping a record of such removals in order to maintain an audit trail;

c) storing all storage media in a safe, secure environment according to their information classification and protecting them against environmental threats (such as heat, moisture, humidity, electronic field or ageing), in accordance with manufacturers' specifications;

d) if information confidentiality or integrity are important considerations, using cryptographic techniques to protect information on removable storage media;

e) to mitigate the risk of storage media degrading while stored information is still needed, transferring the information to fresh storage media before becoming unreadable;

f) storing multiple copies of valuable information on separate storage media to further reduce the risk of coincidental information damage or loss;

g) considering the registration of removable storage media to limit the chance for information loss;

h) only enabling removable storage media ports [e.g. secure digital (SD) card slots and universal serial bus (USB) ports] if there is an organizational reason for their use;

i) where there is a need to use removable storage media, monitoring the transfer of information to such storage media;

j) information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending storage media via the postal service or via courier.

In this control, media includes paper documents. When transferring physical storage media, apply security measures in 5.14.

Secure reuse or disposal

Procedures for the secure reuse or disposal of storage media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

a) if storage media containing confidential information need to be reused within the organization, securely deleting data or formatting the storage media before reuse (see 8.10);

b) disposing of storage media containing confidential information securely when not needed anymore (e.g. by destroying, shredding or securely deleting the content);

c) having procedures in place to identify the items that can require secure disposal;

d) many organizations offer collection and disposal services for storage media. Care should be taken in selecting a suitable external party supplier with adequate controls and experience;

e) logging the disposal of sensitive items in order to maintain an audit trail;

f) when accumulating storage media for disposal, giving consideration to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

A risk assessment should be performed on damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded (see 7.14).

Other information

When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered.

7.11 Supporting utilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

Control

Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

Purpose

To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

Guidance

Organizations depend on utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) to support their information processing facilities. Therefore, the organization should:

a) ensure equipment supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications;

b) ensure utilities are appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;

c) ensure equipment supporting the utilities is inspected and tested regularly to ensure their proper functioning;

d) if necessary, raise alarms to detect utilities malfunctions;

e) if necessary, ensure utilities have multiple feeds with diverse physical routing;

f) ensure equipment supporting the utilities is on a separate network from the information processing facilities if connected to a network;

g) ensure equipment supporting the utilities is connected to the internet only when needed and only in a secure manner.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms. Emergency contact details should be recorded and available to personnel in the event of an outage.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

7.12 Cabling security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection

Control

Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

Guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities being underground where possible, or subject to adequate alternative protection, such as floor cable protector and utility pole; if cables are underground, protecting them from accidental cuts (e.g. with armoured conduits or signals of presence);

b) segregating power cables from communications cables to prevent interference;

c) for sensitive or critical systems, further controls to consider include:

   1) installation of armoured conduit and locked rooms or boxes and alarms at inspection and termination points;

   2) use of electromagnetic shielding to protect the cables;

   3) periodical technical sweeps and physical inspections to detect unauthorized devices being attached to the cables;

   4) controlled access to patch panels and cable rooms (e.g. with mechanical keys or PINs);

   5) use of fibre-optic cables;

d) labelling cables at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Specialist advice should be sought on how to manage risks arising from cabling incidents or malfunctions.

Other information

Sometimes power and telecommunications cabling are shared resources for more than one organization occupying co-located premises.

7.13 Equipment maintenance

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

Control

Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

Guidance

The following guidelines for equipment maintenance should be considered:

a) maintaining equipment in accordance with the supplier's recommended service frequency and specifications;

b) implementing and monitoring of a maintenance programme by the organization;

c) only authorized maintenance personnel carrying out repairs and maintenance on equipment;

d) keeping records of all suspected or actual faults, and of all preventive and corrective maintenance;

e) implementing appropriate controls when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; subjecting the maintenance personnel to a suitable confidentiality agreement;

f) supervising maintenance personnel when carrying out maintenance on site;

g) authorizing and controlling access for remote maintenance;

h) applying security measures for assets off-premises (see 7.9) if equipment containing information is taken off premises for maintenance;

i) complying with all maintenance requirements imposed by insurance;

j) before putting equipment back into operation after maintenance, inspecting it to ensure that the equipment has not been tampered with and is functioning properly;

k) applying measures for secure disposal or re-use of equipment (see 7.14) if it is determined that equipment is to be disposed of.

Other information

Equipment includes technical components of information processing facilities, uninterruptible power supply (UPS) and batteries, power generators, power alternators and converters, physical intrusion detection systems and alarms, smoke detectors, fire extinguishers, air conditioning and lifts.

7.14 Secure disposal or re-use of equipment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection

Control

Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Purpose

To prevent leakage of information from equipment to be disposed or re-used.

Guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete function. See 7.10 for detailed guidance on secure disposal of storage media and 8.10 for guidance on information deletion.

Labels and markings identifying the organization or indicating the classification, owner, system or network, should be removed prior to disposal, including reselling or donating to charity.

The organization should consider the removal of security controls such as access controls or surveillance equipment at the end of lease or when moving out of premises. This depends on factors such as:

a) its lease agreement to return the facility to original condition;

b) minimizing the risk of leaving systems with sensitive information on them for the next tenant (e.g. user access lists, video or image files);

c) the ability to reuse the controls at the next facility.

Other information

Damaged equipment containing storage media can require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk deletion, full-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files);

b) the cryptographic keys are long enough to resist brute force attacks;

c) the cryptographic keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on cryptography, see 8.24.

Techniques for securely overwriting storage media differ according to the storage media technology and the classification level of the information on the storage media. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

See ISO/IEC 27040 for detail on methods for sanitizing storage media.

8 Technological controls

8.1 User endpoint devices

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control

Information stored on, processed by or accessible via user endpoint devices should be protected.

Purpose

To protect information against the risks introduced by using user endpoint devices.

Guidance

General

The organization should establish a topic-specific policy on secure configuration and handling of user endpoint devices. The topic-specific policy should be communicated to all relevant personnel and consider the following:

a) the type of information and the classification level that the user endpoint devices can handle, process, store or support;

b) registration of user endpoint devices;

c) requirements for physical protection;

d) restriction of software installation (e.g. remotely controlled by system administrators);

e) requirements for user endpoint device software (including software versions) and for applying updates (e.g. active automatic updating);

f) rules for connection to information services, public networks or any other network off premises (e.g. requiring the use of personal firewall);

g) access controls;

h) storage device encryption;

i) protection against malware;

j) remote disabling, deletion or lockout;

k) backups;

l) usage of web services and web applications;

m) end user behaviour analytics (see 8.16);

n) the use of removable devices, including removable memory devices, and the possibility of disabling physical ports (e.g. USB ports);

o) the use of partitioning capabilities, if supported by the user endpoint device, which can securely separate the organization's information and other associated assets (e.g. software) from other information and other associated assets on the device.

Consideration should be given as to whether certain information is so sensitive that it can only be accessed via user endpoint devices, but not stored on such devices. In such cases, additional technical safeguards can be required on the device. For example, ensuring that downloading files for offline working is disabled and that local storage such as SD card is disabled.

As far as possible, the recommendations on this control should be enforced through configuration management (see 8.9) or automated tools.

User responsibility

All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures. Users should be advised to:

a) log-off active sessions and terminate services when no longer needed;

b) protect user endpoint devices from unauthorized use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use; not leave devices carrying important, sensitive or critical business information unattended;

c) use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g. avoid reading confidential information if people can read from the back, use privacy screen filters);

d) physically protect user endpoint devices against theft (e.g. in cars and other forms of transport, hotel rooms, conference centres and meeting places).

A specific procedure taking into account legal, statutory, regulatory, contractual (including insurance) and other security requirements of the organization should be established for cases of theft or loss of user endpoint devices.

Use of personal devices

Where the organization allows the use of personal devices (sometimes known as BYOD), in addition to the guidance given in this control, the following should be considered:

a) separation of personal and business use of the devices, including using software to support such separation and protect business data on a private device;

b) providing access to business information only after users have acknowledged their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. In such cases, PII protection legislation should be considered;

c) topic-specific policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;