Physical and Environmental Security Policy

Document version	1
Drafted by	ISMS Working Group/ KOSI
Responsibility for this policy in City of Dublin ETB	Director of OSD
Reviewed by Senior Leadership Team (SLT)	23/01/2024
Approved by Chief Executive	23/01/2024
Noted by Board	15/02/2024
To be reviewed	23/01/2026

1.1 Statement of Intent

The purpose of this policy is to secure physical and environmental areas and to prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities including equipment and personnel.

In summary, the policy requires the following to be protected:

- Physical buildings in which information is stored or processed
- Sensitive paper records
- IT equipment used to access electronic data
- IT equipment used to access the City of Dublin ETB network

Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including personnel and information security. A balanced security program must include a solid physical security foundation. A solid physical security foundation protects and preserves information, physical assets, and human assets.

The protection required needs to be appropriate to the level of information held and the consequential risks of unauthorised access. Each Department is responsible for assessing the level of protection required for their teams and locations.

1.2 Scope

This policy applies to all users who work within City of Dublin ETB schools, training centres or offices or who use any equipment belonging to City of Dublin ETB. The policy defines what paper and electronic information belonging to City of Dublin ETB should be protected and, offers guidance on how such protection can be achieved. This policy also describes employee roles and the contribution staff make to the safe and secure use of City of Dublin ETB information.

1.3 Computer Room Policy

Servers or critical ICT infrastructure and equipment must be stored in a suitable computer room located within a secure area and protected by appropriate security controls. A risk assessment should identify the appropriate level of protection to be implemented to secure the infrastructure and equipment such as:

- Physical Servers
- Networks and Network Devices (firewalls, switches, routers etc…)

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have appropriate control mechanisms in place for the type of information and equipment that is stored there, these could include:

- Alarms fitted and activated outside working hours
- Window and door locks
- Protection against damage e.g. fire, flood, vandalism

As an example, access to secure areas such as the computer room, must be adequately controlled and physical access to buildings should be restricted to authorised persons.

Staff working in secure areas should be ready to challenge anyone not known to them. Each department must ensure that doors and windows are properly secured. Keys, (should be signed for/regularly audited) alarm codes etc. must only be held by staff authorised to access those areas and should not be loaned / provided to anyone else.

1.4 Secure Locations Policy

Critical or sensitive information must be stored in secure areas protected by appropriate security controls. A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored. Examples of secure areas for protection are:

- A room with sensitive paper based information,
- A room with desktop computers used by network or system administrators

1.5 Paper Based Data Security Policy

Paper based (or similar non-electronic) information must be assigned an owner and a classification. If it is classified as personal or confidential, information security controls to protect it must be put in place. A risk assessment should identify the appropriate level of protection for the information being stored. Paper in an open office must be protected by the controls for the building in secure areas and other appropriate measures that could include:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes
- Stored in a Secure Area protected by access controls

1.6 Equipment Security Policy

All general computer equipment must be located in suitable physical locations that:

- Reduce risks from environmental hazards, for example, heat, fire, smoke, water, dust and vibration.
- Reduce the risk of theft, for example, if necessary items such as laptops should be physically attached to the desk
- Facilitate workstations handling sensitive data being positioned so as to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs must not have sensitive data stored on the local hard drive; data must be stored on the network file servers. This ensures that information lost, stolen or damaged via unauthorised access can be restored with its integrity maintained.

All servers located outside of the computer room must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from Information Services. All items of equipment which store or process data or information must be recorded in the information asset register.

Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of. All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the information asset register.

1.7 Cabling Security Policy

Cables that carry data or support key information services must be protected from interception or damage. Power cables should be separated from network cables to prevent interference. Network cables should be protected by conduit and where possible avoid routes through public areas.

1.8 Policy Compliance

All City of Dublin ETB employees, contractors and partners and / or consultants, external individuals and organisations authorised to access City of Dublin ETB's facilities are required to familiarise themselves with this policy and supporting documents, and to adhere to them in the working environment.

Any employee found to have violated this policy may be subjected to disciplinary action.