Information 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 by	23/01/2026

1.1 Statement of Intent

The purpose of this policy is to ensure all information held by City of Dublin ETB, in all formats, which represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.

1.2 Scope

This policy applies to all employees, learners, contractors and partners and / or consultants, external individuals and organisations who interact with information held by City of Dublin ETB and the information systems used to store and process it. This includes, but is not limited to: any systems or data attached to the City of Dublin ETB data or telephone networks, systems managed by City of Dublin ETB, mobile devices used to connect to City of Dublin ETB networks or hold City of Dublin ETB data, data over which City of Dublin ETB holds the intellectual property rights, data over which City of Dublin ETB is the data controller or data processor, electronic communications sent from City of Dublin ETB.

1.3 Objectives

The confidentiality, integrity and availability of information are critical to the on-going functioning and good governance of City of Dublin ETB. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for City of Dublin ETB to recover. This information security policy outlines the City of Dublin ETB approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of City of Dublin ETB's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details. City of Dublin ETB is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all the physical and electronic information assets for which City of Dublin ETB is responsible.

1.4 Information Security Principles

The following information security principles provide overarching governance for the security and management of information at City of Dublin ETB.

- Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Section 1.6. Information Classification) and in accordance with relevant legislative, regulatory and contractual requirements (see Section 1.5. Legal and Regulatory Obligations).
- Staff with particular responsibilities for information (see Section Responsibilities) must:
    1. ensure the classification of that information is established;
    2. must handle that information in accordance with its classification level;
    3. must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities;
- All users covered by the scope of this policy (see Section 1.2. Scope) must handle information appropriately and in accordance with its classification level.
- Information should be both secure and available to those with a legitimate need for access in accordance with its classification level.

a. Access to information will be on the basis of least privilege and need to know.

- Information will be protected against unauthorized access and processing in accordance with its classification level.
- Breaches of this policy must be reported (see Sections 1.8 Compliance and 1.9 Incident Handling).
- Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.
- Any explicit Information Security Management Systems (ISMSs) run within City of Dublin ETB will be appraised and adjusted through the principles of continuous improvement and aligned to meet the mandatory requirements of the Cyber Security Baseline Standards.

1.5 Legal & Regulatory Obligations

Some aspects of information security are governed by legislation, the most notable Irish Acts and European legislation are listed below (See Appendix A):

- Data Protection Acts 1988 to 2018
- Safety, Health and Welfare at Work Act 2005
- Copyright and Related Rights Act 2000 (as amended)
- Criminal Damage Act 1991 and Criminal Justice (Theft and Fraud Offences) Act 2001
- Child Trafficking and Pornography Act 1998 to 2004
- The Irish Constitution (Implicit right to personal privacy under Article 40.3.1)
- European Convention on Human Rights (Article 8)
- The Lisbon Treaty (Article 16)
- The European Charter on Human Rights (Article 8)
- ePrivacy Regulations 2011 (S.I. 336 of 2011)

1.6 Information Classification

The following table provides a summary of the information classification levels that have been adopted by City of Dublin ETB and which underpin the information security principles defined in this policy.

Data classification levels and examples.

Classification	Description	Examples
Public	This information can be freely accessible to all members of the public	• Annual Reports • Corporate Strategy Reports • Website Data
Restricted	This information can be made available to any City of Dublin ETB employees but should not be accessible to members of the public	• Email • Business Data and Information • Systems

		• Company Policy and Procedures
Confidential	This information should be accessible only to specified City of Dublin ETB employees or board members and should be protected against unauthorized disclosure.	• Personal Data (information that identifies living individuals including home / work address, age, telephone number, schools attended, photographs); • Human Resource Data • Financial Data

1.7 Suppliers

All City of Dublin ETB's suppliers will abide by City of Dublin ETB's Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- when accessing or processing City of Dublin ETB assets, whether on site or remotely;
- when subcontracting to other suppliers;

1.8 Compliance, Policy Awareness and Disciplinary Procedures

1. Any security breach of City of Dublin ETB's information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems.
2. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes City of Dublin ETB's Data Protection Policy and may result in criminal or civil action against City of Dublin ETB.
3. The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against City of Dublin ETB. Therefore it is crucial that all users of City of Dublin ETB's information systems adhere to this Information Security Policy and its supporting policies as well as the Information Classification adopted by City of Dublin ETB.
4. All City of Dublin ETB employees and other authorised users will be informed of the existence of this policy and the availability of supporting policies, processes and guidelines.
5. Any security breach will be handled in accordance with all relevant policies, including the Acceptable of Use of IT and Data Protection Policies as well as the appropriate disciplinary policies.

1.9 Incident Handling

1. If any City of Dublin ETB employee is aware of an information security incident then they must report it to the Information Security Officer/ Data Protection Officer.
2. Breaches of personal data will be reported to the Information Commissioner's Office by City of Dublin ETB's Information Security Officer/ Data Protection Officer.

1.10 Supporting Policies, Procedures and Guidelines

Information security is considered as safeguarding three main objectives:

- **Confidentiality**: Data and information assets must be confined to people who have authorised access and not disclosed to others
- **Integrity**: Keeping the data intact, complete and accurate, and IT systems operational
- **Availability**: An objective indicating that information or system is at disposal of authorized users when needed.

The Information Security Policy must be read in conjunction with other IT Policies, including:

- Acceptable Use of IT Policy
- Access Control Policy
- Data Protection Policy
- Firewall Policy
- Password Policy
- Clear Desk / Screen Policy
- Remote Working Policy

All City of Dublin ETB employees, contractors and partners and / or consultants, external individuals and organisations authorised to access City of Dublin ETB’s network or computing 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.