ICT Backup and Restore Policy

Document version	V 1.0
Drafted by	ETBI ICT Group
Responsibility for this policy in City of Dublin ETB	Director OSD/Head of IT
Reviewed by Senior Leadership Team (SLT)	24/09/2024
Approved by Chief Executive	24/09/2024
Noted by Board	22/10/2024
To be reviewed	1 year from date of approval by CE

Contents

1 Introduction

1.1 Purpose of this Document

The Backup and Restore Policy is defined in the City of Dublin ETB ICT Framework Policy and should be read in conjunction with all other ICT policies to ensure required security standards are adhered to. The purpose of this policy is to define the activities associated with the provision of data backup and recovery plans and programs that protect City of Dublin ETB information systems, networks, data, databases, and other information assets.

1.2 Scope and Constraints

The scope of this backup and recovery policy is all information technology systems, software, databases, applications, and network/security resources needed by City of Dublin ETB to conduct its business.

1.3 Definitions

A full range of definitions is available in the ICT Frameworks Policy

1.4 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, who are committed to continually improving the protection of all City of Dublin ETB information assets and the protection of personal data where City of Dublin ETB is a controller or processor. This document will be reviewed at least annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within the organisation.

2 Backup and Restore Policy / ICT responsibility

ICT Department will ensure that regular backups are performed in line with Asset Owner requirements as appropriate.

This policy covers all business applications and the data generated including all databases and folders, all digital assets and all data relevant to City of Dublin ETB business operations both on the local admin networks and cloud hosted platforms.

It does not cover data generated by students both on school workstations or on local servers used for student education purposes.

All information and data which City of Dublin ETB is responsible for shall be protected against loss or corruption through the use of robust backup procedures. These procedures will be performed with sufficient frequency to ensure that the organisation is not significantly disrupted should a failure occur within the systems.

Adequate back-up facilities shall be provided to ensure that all essential business information and software can be recovered following a disaster or media failure.

Back-up arrangements for individual systems and related data shall be tested according to a formal schedule to ensure that they meet the requirements of business continuity plans.

All Servers hosting City of Dublin ETB systems and data should be backed up.

Backup selection lists should be documented identifying the systems and data being backed up and purpose. Systems to be backed up include but are not limited to:

- File servers
- Terminal servers
- Databases
- Domain controllers
- Virtual Server image
- Full backup weekly
- Full incremental backups to be made nightly
- Retention to provide 5 daily restore points, 3 weekly and 12 monthly

Backup

The following must be considered when making backups:

- The need to keep backup copies and associated procedures in a different place from where the systems which process such information are found;
- The need to encrypt information with backup;
- The need to encrypt back-up data where the original information is encrypted. The encryption can be through the backup copying system or the information can be stored in encrypted format. The encryption keys and associated programmes must be stored separately so that the data can be retrieved using the encryption information if necessary;
- The need to check backup copies periodically and on a rota basis abiding by predefined testing schedules, using a verification tool or retrieving part of the set, in order to guarantee that the copies are available when needed;
- Backup copies should be made in such a way that they permit individual file/folder retrieval as well as entire system retrieval from the system and the information processed;
- Backup copy-making procedures should be automated, making the task easier for operators and preventing possible errors in copy handling;
- Wherever necessary, a backup copy of the information and copy of the retrieval procedure should be kept in a different place from that where the data processing systems are found. Such location should comply with all the security measures applied to the original location or should feature elements which guarantee the integrity and retrieval of the information, making its recovery possible;
- The correct definition, running and application of the backup copy and retrieval procedure should be checked periodically. This verification should be carried out at least every 6 months.

Retrieval

- The recovery of information from backup copies must be authorised by the asset owner.

The backup system installed should not depend on itself for its own retrieval.

Where backups are created, the following information must be included in a *documented and formalised backup and recovery plan:*

General Information	• the person(s) responsible for making the backup copies and for their custody • the frequency of backup copies • the number of copies • the type of backup (complete or differential/incremental) • maximum storage times (expiry dates) and whether it is necessary to delete the information once expiry date is reached (as well as the type of destruction required) • acceptable minimum times for information retrieval
Backup Information	• register(s) of the copies made • retrieval procedures
Recovery Information	• recovery actions • the people executing the process • the authorisation for recovery • the information restored • the reason for recovery • the validation processes associated with the operation and the acceptance on the part of the asset owner of the recovered information or system. This should guarantee the reconstruction of the information in the same status as it was at the time of the loss or destruction, according to the retrieval times established and agreed with its asset owner.

- The data backup and recovery plan must be kept up-to-date that reflects the changes to the updated environment.
- It is established good practice to keep a full set of backup media stored offsite. In the event of normal backup and restore devices being unavailable due to fire for example, it is imperative that alternative backups are available in a separate location.

- One copy of each backup should be air gapped or immutable storage that cannot be accessed by any compromised systems such as ransomware attacks. Should a ransomware attack succeed, a full backup copy should be guaranteed to be available for recovery.
- Backup documentation should include the name of each backup job

3 Users responsibilities

Users should notify the ICT helpdesk / asset owner immediately upon discovering a possible need to restore data.

Users should ensure all information is stored appropriately to ensure work related information is backed up and can be restored when required.

Users must store work information in the appropriate location as identified by ICT dept to facilitate successful backup of information.

4 Enforcement

Individuals found to be in breach of this policy, may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

5 References

ISO27001	NIST CSF	PCI-DSS