[Company]

BACKUP POLICY

Management of Backups

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Backup Policy

3.1 Purpose

The purpose of this policy is to protect against loss of data and enable recovery from loss of data or systems.

3.2 Scope

All employees and third-party users.

Company owned, managed, and controlled information and systems that form part of systems and applications deemed in scope by the ISO 27001 scope statement including:

- Servers
- Databases
- Code Repositories
- Test Environments
- Development Environments

Out of scope for back up:

- Desktop
- Laptop
- Mobile Device

3.3 Principle

Information is backed up securely in line with the

- data retention requirements
- business requirements
- business continuity requirements and plans
- business impact assessment
- legal and all legal and regulation legislation requirements including but not limited to the GDPR and Data Protection Act 2018.

3.4 Backup Restoration Procedures

Backup and restoration procedures are documented, in place and maintained.

3.5 Backup Security

Backups are encrypted using vendor built in encryption.

Backups are stored in cloud-based solutions that as a minimum are ISO 27001 certified.

Where backup is to physical media

- The media is encrypted
- The media is labelled and stored securely on site with restricted, authorisation required perimeter access control.

- The media is transferred by and approved third party secure courier and stored in a remote secure location.

3.6 Backup Schedule

A backup schedule, retention schedule and testing schedule are available and summarised as

- Daily back-ups are maintained for 7 days.
- Weekly back-ups are maintained for 28 days.
- Monthly back-ups are maintained for 12 months.

3.7 Backup Testing and Verification

Backups of systems are tested at least annually to ensure they can be relied upon in an emergency and meet the needs of the business continuity plans and business requirements.

Backup logs are produced and checked for errors and performance at least weekly. Where errors are found corrective action is taken.

Backup testing log reviews are recorded.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.