Information Security and Data Protection Policy (Public Version)

Effective Date: 28 May 2025
Version: 1.8

Introduction

At Talk Think Do, we are committed to safeguarding the confidentiality, integrity, and availability of the data we hold. This policy provides an overview of how we protect our systems, services, and data in accordance with ISO 27001:2022 and the UK General Data Protection Regulation (UK GDPR).

This version is designed for transparency with our clients, partners, and the public, summarising the controls we have in place while omitting sensitive internal operational detail.

Our Objectives

- Protect the information assets we store, process, or access.
- Ensure controls are proportionate to risk and value.
- Comply with legal, contractual, and regulatory obligations.
- Continuously improve our Information Security Management System (ISMS).

Scope

This policy covers:

- All employees, contractors, and third parties accessing our systems.
- Our infrastructure, including cloud services, mobile devices, and software.
- All data types, including customer, personal, confidential, and operational data.

Core Policy Areas

1. Acceptable Use of Assets

All users must:

- Only access systems for legitimate business purposes.
- Avoid unauthorised software or external devices.
- Never share passwords or allow unauthorised system access.
- Use corporate communication tools responsibly, e.g., email, Teams.

2. Access Control

- Role-based access is granted and reviewed regularly.

- All accounts use multi-factor authentication where possible.
- Access logs are monitored to detect unauthorised use.
- Leaver access is revoked immediately upon termination.

3. Data Protection (UK GDPR)

We apply data protection principles to all personal data:

- Data is collected and used lawfully, with clear purpose.
- We minimise the data we collect and limit retention.
- Individuals can request access, rectification, deletion, or restriction.
- Privacy notices are provided for all data subjects.

4. Backup and Recovery

- Daily encrypted backups are stored securely in cloud infrastructure.
- Backups include system state, user files, and databases.
- Backup integrity is tested at least annually.
- Recovery procedures support our Business Continuity Plan.

5. Mobile and Remote Work

- All corporate devices are enrolled in Microsoft Intune.
- Remote access is protected by VPNs and timeouts.
- Personally owned devices must meet strict configuration standards.
- Data must not be stored locally unless approved.

6. Information Classification

- Data is categorised as Public, Internal, or Confidential.
- Labels are applied to electronic and physical records.
- Access and distribution controls are based on classification.

7. Encryption and Cryptography

- Data in transit and at rest is encrypted using industry standards.
- BitLocker is enforced for endpoint encryption.
- Encryption keys are securely stored and access controlled.

8. Physical Security

While we are currently a remote-first company, physical controls apply to any location where information is stored:

- Access to physical sites is restricted and logged.
- Devices must not be left unattended in unsecured environments.

9. Malware Protection

- All endpoints run Microsoft Defender for Endpoint with real-time protection.
- Web filtering prevents access to known malicious sites.
- Software updates and patches are applied automatically.

10. Clear Desk and Screen

- Devices lock after 5-15 minutes of inactivity.
- Printed materials are stored securely when unattended.
- Screens must be obscured when not in use.

11. Threat Intelligence and Monitoring

- We monitor for emerging threats through cyber intelligence forums.
- Our Founder and technical leads assess and act on new vulnerabilities.
- Security improvements are tracked via an internal improvement log.

12. Incident Management

- All security incidents are reported immediately to senior management.
- We have a defined response plan, aligned to ISO 27001.
- Personal data breaches are reported to the ICO within 72 hours if required.

13. Third-Party and Supplier Security

- All suppliers handling sensitive data sign data protection and security terms.
- Cloud services must meet our requirements for security, jurisdiction, and resilience.
- Periodic reviews and audits are performed to assess supplier compliance.

14. Data Retention

- All data types have documented retention periods.
- Once expired, data is securely deleted or anonymised.
- Backups are reviewed for expiry compliance.

Governance and Oversight

- **Managing Director**: Responsible for ISMS and compliance.
- **Founder**: Oversees risk management, encryption, and remote access controls.
- **Project Management Office (PMO)**: Maintains records, handles data requests, and provides training.
- All employees are expected to report security incidents and comply with this policy.

Certification and Standards

- Our ISMS is certified to ISO 27001:2022.

- We comply with the UK GDPR and Data Protection Act 2018.
- Our software, infrastructure, and supplier relationships are designed with security and privacy by design.

Contact

To learn more or to exercise your data rights:

Email: louise.clayton@talkthinkdo.com

Phone: +44 1202 006729
Postal Address: 7-8 Church Street, Wimborne, England, BH21 1JH

This policy is reviewed at least annually or following significant changes to our services or regulatory requirements.