Midway TS - Data Protection Policy (ISO 27001)

1. Purpose

The purpose of this policy is to ensure that all personal, confidential, and business data managed by the organisation is protected from unauthorised access, disclosure, alteration, or destruction.

This policy sets out clear principles for responsible data management, maintaining trust, and ensuring compliance with all relevant data protection and privacy requirements.

2. Scope

This policy applies to all employees, contractors, and third parties who collect, store, process, or access company data in any format, whether digital or physical.

It covers all data managed by the organisation, including customer information, employee records, financial data, intellectual property, and business operations data.

The policy applies to all locations, systems, devices, and cloud services used to process company data.

3. Definitions

Personal data: Any information that can directly or indirectly identify an individual, such as a name, email address, or contact details.

Confidential data: Information not publicly available that could harm the organisation, its customers, or partners if disclosed.

Data processing: Any action performed on data, including collection, storage, use, transmission, or deletion.

Data subject: Any individual whose personal data is collected or processed by the organisation.

Data breach: Any incident resulting in unauthorised access to, or loss of, personal or confidential data.

Special category data: Sensitive personal information that needs extra protection, including health details, beliefs, sexual orientation, and information about young people.

4. Policy Statement

The organisation is committed to protecting data throughout its lifecycle by implementing appropriate technical and organisational safeguards.
All data processing activities must align with the organisation's Information Security Management System (ISMS) and support the confidentiality, integrity, and availability of information assets.

5. Policy Requirements

5.1 Data Protection Principles

All data must be:

- Collected lawfully and fairly for legitimate business purposes.
- Used only for the purposes for which it was collected and not further processed in a way that's incompatible with those purposes.
- Limited to what's necessary—avoid collecting or storing excessive information.
- Accurate and kept up to date whenever possible.
- Stored securely and protected against unauthorised or unlawful access, alteration, or loss.
- Retained only as long as needed for business, legal, or contractual requirements.
- Securely disposed of when no longer required.

5.2 Data Classification

Data must be classified based on its sensitivity and importance to the organisation, such as: Public, Internal, Confidential, or Highly Confidential.
The assigned classification determines how data is handled, stored, and shared.
Employees must understand and follow the handling requirements appropriate to each data classification level.

5.3 Data Access and Use

Access to data must follow the principle of least privilege—only authorised individuals may access the data necessary for their role.
Confidential and personal data must only be shared using approved, secure channels.
Personal email accounts or unauthorised storage services must not be used for company data.
Employees must not copy data to removable media unless specifically authorised and encrypted.

5.4 Data Storage and Security

All systems that store data must have appropriate security measures, such as encryption, access controls, and regular backups.
Data stored in cloud services must use approved providers that meet the organisation's security standards.
Portable devices containing company data must be encrypted and protected by passwords or other access controls.
Physical records containing personal or confidential data must be stored in locked cabinets or other secure locations.

5.5 Data Retention and Disposal

Data must only be kept as long as necessary to meet operational, contractual, or legal obligations.
When data is no longer needed, it must be securely deleted, shredded, or otherwise destroyed.
Retention periods must be documented in a data retention schedule and reviewed regularly by management.

5.6 Data Breaches and Incident Management

Any suspected or actual data breach must be reported immediately to management and Lisa Phillips, Data

Protection Officer.
All data breaches will be investigated, documented, and addressed in accordance with the organisation's Security Incident Response Policy.
When required by law or contract, affected parties will be notified promptly.
Lessons learned from incidents must be used to improve future data protection measures.

5.7 Third-Party Data Processing

Third parties or service providers that process company data must have adequate security and privacy controls in place.
Contracts or agreements must clearly define data protection responsibilities, confidentiality obligations, and breach notification requirements.
Third-party access must be reviewed regularly and revoked when no longer needed.

5.8 Employee Responsibilities

Employees must handle all data responsibly and in accordance with this policy.
Data must not be disclosed to unauthorised individuals, either inside or outside the organisation.
Employees are required to complete all mandatory data protection and information security awareness training.
Any suspected data loss, unauthorised access, or disclosure must be reported immediately.

6. Roles and Responsibilities

6.1 Management

Responsible for ensuring data protection practices are implemented, allocating the necessary resources, and maintaining compliance.

6.2 IT Lead or System Administrator

Responsible for implementing technical controls for data security, access management, backups, and encryption.

6.3 Employees and Contractors

Responsible for handling data securely, following policy requirements, and promptly reporting any issues or incidents.

6.4 DPO

Responsible for handling data securely, following policy requirements, and promptly reporting any issues or incidents and investigating any data breaches and incidents, liaising with the ICO. DPO is responsible for overseeing data protection compliance and safeguarding personal data. Responsible for all DIPAs within the company.

7. Compliance

Compliance with this policy is mandatory. Violations may result in disciplinary action, loss of access, or legal consequences.
The organisation may audit data handling and access logs to ensure compliance with this policy.
This policy supports compliance with **ISO 27001: 2022** controls, including:

- A.5.10 – Acceptable use of information and associated assets
- A.5.12 – Classification of information
- A.5.32 – Protection of records
- A.5.33 – Privacy and protection of personally identifiable information (PII)
- A.5.34 – Information security in supplier relationships
- A.5.35 – Protection of data in transit
- A.5.36 – Protection of data at rest

This policy will be reviewed annually, or whenever there are significant changes in technology, operations, or legal requirements, to ensure it remains effective and relevant.

Monitoring and review

Midway Transitional Solutions reserves the right to regularly review the operation of

this policy at any point and as they see fit