

PDF Sample INFORMATION SECURITY POLICY

Purpose, scope and users

The aim of this Policy is to define the purpose, direction, principles and basic rules for information security management.

This Policy is applied to the entire **GDPR** as defined in the GDPR Scope Document.

Users of this document are all employees ofLtd, as well as relevant external parties.

Commented [dk1]: Complete all yellow highlighted areas with relevant information

1. Reference documents

- **GDPR** Scope Document
- Risk Assessment & Treatment
- **GDPR** Logs
- List of Legal, Regulatory and Contractual Obligations
- **GDPR** Data Breach Response and Notification Procedure

2. Basic information security terminology

Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.

Integrity – characteristic of the information by which it is changed only by authorized persons or systems in a permissible format.

Availability – characteristic of the information by which it can be accessed by authorized persons.

Information security – preservation of confidentiality, integrity and accessibility of information.

Information Security Management System – part of overall management processes that takes care of planning, implementing, maintaining, reviewing, and improving the information security.

3. Managing the information security

Commented [dk2]: Keep objectives uncomplicated, but ensure key elements have been captured and are workable and monitor via management meetings and recorded in the minutes

3.1. Objectives and measurement

General and individual security controls objectives for the information security management system are the following: creating a better market image and reducing the damage caused by potential incidents and compliance with the **GDPR**; goals are in line with the business objectives, strategy and business plans. **Managing Director** and **Senior Management Team** are responsible for reviewing these objectives and setting new ones. All the objectives must be reviewed at least once a year.

.....Ltd will measure the fulfilment of all the objectives. **Managing Director** and **Senior Management Team** are responsible for setting the methods for measuring the achievement of the

objectives – the measurements will be performed at least once a year and will analyse and evaluate the measurement results, report them as input materials for the **Management Review Meeting**. The business should record the details and results in the business **M.R.M.**

3.2. Information security requirements

This Policy and the entire **GDPR** must be compliant with legal and regulatory requirements relevant to the business in the field of information security and personal data protection, along with the contractual obligations.

3.3. Information security controls

The process of selecting the controls/safeguards is defined in the Risk Assessment Treatment plan.

Selected controls and their implementation status should be listed in the Records.

3.4. Responsibilities

Responsibilities for the GDPR are the following:

- **Managing Director** is responsible for ensuring that the **GDPR** is implemented and maintained according to this Policy, and for ensuring all necessary resources are available
- **Managing Director** is responsible for operational coordination of the **GDPR** and personal data protection as well as for reporting about the performance of the **GDPR**. If appointed the Data Protection Officer is responsible for the overall compliance of personal data processing with the **GDPR**; detailed roles and responsibilities are described in the document Data Protection Officer Job Description.
- Management must review the **GDPR** at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy and effectiveness of the **GDPR**.
- **Managing Director** will implement training and awareness programs for employees
- the protection of integrity, availability, and confidentiality of assets is the responsibility of the owner of each asset
- All data breaches, security incidents or weaknesses to be reported to the **Managing Director**
- **Managing Director** will define which information will be communicated to which interested party (both internal and external), by whom and when
- **Managing Director** is responsible for adopting and implementing the Training Plan, which applies to all persons who have a role in information security management

3.5 Policy communication

Managing Director must ensure that all employees of Ltd as well as appropriate external parties are familiar with this Policy.

Commented [dk3]: Include senior management as part of the whole team if relevant approval has been agreed

Commented [dk4]: This only applies if the position (D.P.O.) has been necessary for the business.

E.G. If the business deals with large public organisation/government/councils or handles large quantities of data or is involved with direct marketing.

If not and or the business is relatively small, then this position is not warranted.

Commented [dk5]: With current or new staff, it's a simple process of signing the Acceptance doc as seen, read and agree.

Suppliers there is a simple process and pre-made out templates to be used to ensure compliance.

However, do consider some external services from suppliers who will also need to be compliant. E.G. External Accounting, HR or IT or Legal services.