**INFORMATION SECURITY POLICY**

Contents

[1 SCOPE 3](#_Toc24619440)

[2 GOVERNANCE 3](#_Toc24619441)

[3 INFORMATION SECURITY INTRODUCTION 3](#_Toc24619442)

[4 RESPONSIBILITIES 4](#_Toc24619443)

[5 information security management 5](#_Toc24619444)

# SCOPE

This policy applies to all employees, directors, consultants and sub-contractors working within or for the organisation. Failure to comply with security policy can lead to unnecessary risk and compromise of information; therefore, violations of this policy may result in legal or disciplinary action if deliberate or wilful neglect has been proven. All policies and guidelines must be read in conjunction with this document and are available on the intranet or at request from the HR function.

# GOVERNANCE

The Information Security Steering Group (ISSG) composed of senior management representatives, is responsible for the explicit authority assignment, acknowledgement of responsibilities, active support and clear direction of the information security function.

Line management are directly responsible for ensuring their staff comply with policies, supporting guidelines and procedures.

Where appropriate, each function is to appoint a Business Information Security Officer, responsible for the awareness and compliance with security policy, standards and guidelines.

All provided information systems are liable to recording and monitoring at any time to maintain adequate security and to ensure that services remain available to end users. Enforcement and measurements for compliance may be accomplished through differing means including audit, management review, technical assessment and techniques to identity unauthorised attempts to manipulate or change information.

# INFORMATION SECURITY INTRODUCTION

The purpose of the information security functions is to protect information assets from all threats, whether internal, external, accidental or deliberate and can only be achieved with full cooperation.

Information security includes information classification, risk management, policy, education and awareness. These activities serve as the fundamentals.

There are three key attributes to information security:

* **Confidentiality** – to protect information from unauthorised disclosure.
* **Integrity** – to safeguard the accuracy and completeness of information.
* **Availability** – to ensure the timely availability of information to authorised staff.

Information consists of many types and forms including that which is stored on PCs and laptops, transmitted by eMail, stored on hard drives, USB sticks, in cupboards or even spoken in conversation or over telephone. To enable adequate security all information needs to be identified, clearly owned and classified.

# RESPONSIBILITIES

We are all responsible for the following:

* **Complying with all information security policies, guidelines and procedures.**

Information security policies, guidelines and procedures related to the protection of information and information systems are published on the intranet.

These include:

|  |  |
| --- | --- |
| **Document** | **Description** |
| **Information Security Policy** (*This document*) | High level overview of information security objectives, assignment of security responsibilities and staff responsibilities. |
| **Data Protection Policy** | Supports the necessity of protecting personal data according to the UK Data Protection Act. |
| **Secure Working Policy** | Provides requirements in terms of acceptable use for:   * Email usage * Internet and instant messaging usage * Working in 3rd party environments * Day-to-day operations |
| **Social Media Policy** | Outlines the requirements which are to be considered in terms of acceptable use of social media. |
| **Information Handling Policy** | Provides requirements for staff to handle the information they are faced with for business purposes and in the context of their roles within the organisation.  This policy provides detail and specific requirements on information classification. |
| **Password Management Standard** | Minimum requirements on the usage of passwords for all systems. |
| **Cryptography Standard** | The Cryptography Standard is a technical document and applies only to those who employ cryptographic functions. This document is created to assist with the selection of appropriate cryptographic controls such as encryption to protect information. |

* **Reporting actual or suspected vulnerabilities or breaches in the confidentiality, integrity or availability of information to the information security team.**

During the course of day-to-day operations, if faced with a situation where the security of information might be at risk, it is to be reported to the information security team as soon as possible. For example, if confidential information has been disclosed on a website that shouldn’t be accessible, that situation needs to be reported. It may be appropriate to notify a local Business Information Security Officer who will support you.

Report security events to: [incidentresponse@your\_organisation.com](http://ncidentresponse@your_organisation.com)

# information security management

The information security policy, supporting standards and guidelines are in place to provide management direction and support for information security activities in accordance with business requirements and relevant laws and regulations.

The following summarises transparency into the information security management system which is operated, monitored, measured and reported upon by the information security team.

|  |  |
| --- | --- |
| **Process** | **Goal** |
| **Organisation** | Business Information Security Officers (BISO) roles are in place, trained, and supported by all staff to deliver their objectives. |
| **Information asset inventories and classification** | Information asset inventories are in place for every department, control assessments thereof performed, and actions are addressed to ensure the protection of information. |
| **Measures to protect information** | Measures are in place and visibly applied by all employees resulting in minimal information security incidents. Retention periods are reviewed, and secure disposal requirements are in place. |
| **Risk management** | Information security risk management approach is fully defined and implemented assessing all relevant risk sources to determine information security risk exposure and remediating actions. |
| **Management awareness** | Regular meetings, presentation, and briefings with management teams are held; reports are issued, reviewed and discussed. |
| **Policy monitoring and enforcement** | All staff complies with security policies, policy updates are performed and communicated following changes to business strategy and new and changing threats. |
| **Education and training** | All staff is provisioned with information security education and awareness training. |
| **Event handling** | Information security events are reported, and weaknesses are handled in a manner allowing timely corrective action. |

These security processes are co-ordinated by the information security team with Business Information Security Officers representing each part of the company.

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Brief description** |
| 0.1 | xx-xxx-xx | xxxxx | First draft |
| 0.2 | xx-xxx-xx | xxxxxx | Updated based on:  xxxxx Directors  Human Resource Directors  Legal Directors  Information Security Management Team  Information Security Steering Group |