Information Security Policy

This is a non-contractual policy

Created: March 2020
Review date: April 2023

Introduction

This information security policy applies to information, systems, networks, applications, locations and staff of Smartdesc. This policy is based on ISO 27001:2013, the International Standard for Information Security.

Aim

The aim of this policy is to enable and maintain effective security and confidentiality of information, information systems, applications and networks owned or held by Smartdesc. This shall be achieved by:

- ensuring that all Smartdesc employees are aware of and shall comply with relevant legislation, including the Data Protection Act 2018 and the UK General Data Protection Regulation
- describing the principles of information security management and how they shall be implemented within Smartdesc
- introducing an approach to information security that is consistent with managed service provider organisations and their expectations of contracted organisations
- assisting employees in identifying and implementing information security as an integral part of their day-to-day role within Smartdesc
- protecting information assets and safeguarding information relating to staff and clients under the control of Smartdesc.

Objectives

The key objectives of this Information Security Policy are to preserve:

- confidentiality - access to information shall be restricted to those staff of Smartdesc and relevant others with agreed authority to view it
- integrity – records are to be complete and accurate with all filing and management systems operating correctly
- availability - information shall be readily available and delivered to the authorised staff member or contracted third party, when it is needed.

Scope

This policy applies to all information, information systems, networks, applications, locations and users of Smartdesc or supplied under contract to it.

Responsibilities for Information Security

Responsibility for information security shall rest with the Smartdesc Directors. However, on a day-to-day basis the Smartdesc Head of Information Security shall be responsible for organising, implementing and managing this policy and its related good working practices.

The Head of Information Security shall be responsible for ensuring that both permanent and temporary staff including any volunteers are aware of:

- the information security policies applicable to their work areas
- their personal responsibilities for information security
- who to ask or approach for further advice on information security matters.

All employees shall abide by the security procedures of Smartdesc. This shall include the maintenance of organisation records whilst ensuring that their confidentiality and integrity are not breached (this applies to client, staff and corporate information). Failure to do so may result in disciplinary action.

This Information Security Policy document shall be owned, maintained, reviewed and updated by the Head of Information Security. This review shall take place annually and will include a review of the overall ISMS and how Information Security is managed. The results of which shall be made known to the Senior Leadership Team.

Employees shall be responsible for the security of their immediate working environments and the security of information systems they use (e.g. workstations, laptops, mobile devices, etc).

Any contracts with third party organisations that allow access to the information systems of Smartdesc, shall be in place before access is allowed. These contracts shall ensure that the staff or sub-contractors of those external organisations shall comply with all the appropriate security policies/guidance required by Smartdesc.

Legislation

Smartdesc is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Smartdesc, who may be held personally accountable for any breaches of information security for which they may be held responsible. Smartdesc shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The UK General Data Protection Regulation (2021)
- The General Data Protection Regulation (2016)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- Human Rights Act (1998)

Policy Framework

Smartdesc shall undertake to ensure:

- The management of Information Security
- at board level, responsibility for information security shall reside with the Directors
- the Head of Information Security shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

Information security awareness training shall be included in the staff induction process. An ongoing awareness programme has been established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Contracts of employment address information security requirements at the recruitment stage and all contracts of employment shall contain a confidentiality clause. The information security requirements shall be included within job descriptions.

Network security is appropriately managed and controlled in order that information that resides or flows within the supporting infrastructure is protected from threats and the security of the systems and applications and any information in transit to external parties is maintained.

Access controls to areas containing information systems are restricted and controlled to ensure that only staff and those authorised can access information managed by the organisation. Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Equipment security is effective in order to minimise losses, or damage to Smartdesc. Where possible, all information assets and equipment shall be physically protected from security threats and environmental hazards. Locked cabinets (fireproof if possible), clear desk policy and the limitation of risks in the surrounding work area etc.

Information risk assessment – a regular assessment of the working environment and information systems shall be conducted to identify potential risks to the security of information. Where risks are identified, these should be noted and where possible mitigating action taken.

Information security incidents and weaknesses are to be recorded and reported via the Security Incident Procedure, so that they can be investigated to establish their cause, impact and effect on Smartdesc and its clients.

Protection from malicious software should be provided by using commercial strength anti-virus/anti-malware software. Where there is an internet connection an appropriate firewall shall be installed and managed. No new software shall be downloaded or installed on computer systems of Smartdesc without the explicit permission of an employee's line manager. Breach of this requirement may be subject to disciplinary action.

User Media - Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the employee's manager before they may be used on Smartdesc systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

Secure Communications – should be in place to ensure that all correspondence, faxes, email, telephone messages and transfer of confidential information are conducted in a secure and confidential manner, this includes the encryption of files that contain sensitive information.

Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the Operations Director before they commence operation.

Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed regularly.
Smartdesc has routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- establishing the existence of facts
- investigating or detecting unauthorised use of the system
- preventing or detecting crime
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- in the interests of national security
- ascertaining compliance with regulatory or self-regulatory practices or procedures
- ensuring the effective operation of the system.
- any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

System Change Control

Changes to information systems, applications or networks shall be reviewed and approved via the change management process.

Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed. Users shall not install software on the organisation's property without the relevant manager's permission. Users breaching this requirement may be subject to disciplinary action.

Business Continuity and Disaster Recovery Plans are in place so that in the event of a disruption to the organisation's information services, it is possible to activate relevant business contingency plans until affected services are restored.

Reporting

The Head of Information Security shall keep the Executive team informed of the organisation's information security status through regular reports and presentations to the Senior Leadership Team.

Further Information

Further information and advice on this policy can be obtained from the Head of Information Security.

Document Control

Security classification	OFFICIAL – NOT MARKED
Author	Andrew Coyle
Owner role	Head of Information Security
Approved by	Head of Information Security
Approval date	17/04/2018
Distribution	All staff via email and intranet. Staff induction
Signature required	No
Latest review date	24/04/2023
Next review date	24/04/2024
References	Data protection act 2018 The UK General Data Protection Regulation 2021 General Data Protection Regulation 2016 ISO 27001 & ISO 27002 Information Security Standard and Code Of Practice

Change History

Version	Owner	Changed by	Change summary	Date
1.0	IT Director	Andrew Coyle, Smartdesc Associate	NEW	19/01/17
1.1	ISM	Andrew Coyle, Information Security Manager	Reviewed	17/04/18
1.2	ISM	Andrew Coyle, Information Security Manager	Reviewed and minor amendments	04/10/2018
1.3	HoIS	Ricci Wilding, Information Governance Officer	Reviewed and minor amendments	25/02/2020
1.4	HoIS	Ricci Wilding, Information Governance Officer	Reviewed and minor amendments	12/01/2021
1.5	HoIS	Kemi Emmanuel, Information Governance Officer	Reviewed and minor amendments	20/05/2022
1.6	HoIS	Ricci Wilding, Information Governance Manager	Brand changes and minor amendments	24/04/2023