Group Information Security Policy

ISMS002

Contents

Standards relevant to this policy

ISO 27001 Control A.5 – Information security policies

A.5.1.1 - Policies for information security
A.5.1.2 - Review of the policies for information security

1. Purpose

The purpose of the Information Security Policy is to describe the information security objectives of The British Standards Institution, together with its subsidiaries ("BSI") for protecting our information assets. An 'information asset' is information held by BSI that is sensitive, confidential or has value to BSI. It includes third party information (such as Client or Supplier data) and BSI's information systems.

2. Scope

BSI information assets are grouped into the following categories:

i. Information (e.g. data, documents, intellectual property, knowledge, application and system software documentation)
ii. IT infrastructure (e.g. laptops, corporate mobiles, tablets, network hardware components)
iii. Application and System Software (e.g. Point Global, Sales Force, Microsoft applications, Remedy)
iv. Premises from which Employees and Contractors ("Personnel") operate or where BSI retains IT infrastructure

(Note: For the purposes of ISMS certification only, refer to the "ISMS050 Scope for the Information Security Management System" document to identify the elements which are currently in the certification scope.)

BSI has established an Information Security Management System (ISMS) framework to support this Policy. The framework consists of policies, processes and procedures supported by both management and technical controls appropriate to the risk profile of BSI.

This Information Security Policy applies to all personnel worldwide. It does not form part of any employee's contract of employment and may be subject to amendment from time to time. All personnel are responsible for compliance with this policy and the framework that underpins it. Managers are responsible for implementing this policy and ensuring compliance within their teams.

3. Information Security Objectives

The following objectives apply across BSI:

i. protect the confidentiality, integrity and availability of BSI's information assets;

ii. provide information with minimal disruption to personnel, suppliers, clients and interested parties, as required by BSI and the appropriate compliance and regulatory framework;

iii. increase client confidence in BSI's ability to protect client information entrusted to it;

iv. protect the reputation of BSI and enhance BSI brand value;

v. reduce the risk of information security breaches, incidents and loss of data and information assets;

vi. comply with data protection laws on the protection of personal data, both as a data controller and as a data processor (See ***Privacy Policy*** for further information);

vii. reduce the risk of personal data breaches and protect the rights of data subjects (See ***Privacy Policy*** for further information);

viii. increase personnel and supplier awareness to information security threats;

ix. recognise BSI expertise in applying management systems by gaining third party recognition of the ISMS; and

x. provide a structured approach to securing information, led by senior management who are committed to continual improvement of the ISMS.

The methods of evaluating measurable objectives are set out in Appendix A.

4. Intent of the ISMS

All personnel are responsible for ensuring the safety of BSI information assets.

The BSI Board and Group Executive support the information security objectives and an Information Security Steering Committee ("ISSC") has been established to oversee the achievement of these objectives. The Chief Executive Officer is Chair of the ISSC, while the General Counsel is responsible for the implementation and deployment of the ISMS across BSI. A Group Information Security Officer has been appointed to be responsible for defining, managing and ensuring compliance with the ISMS.

BSI commits that it will:

i. take a risk-based approach to managing information assets in order to minimise the risk of information security breaches;

ii. allocate resources, responsibility and authority which will be regularly reviewed by Executive Management to ensure the ongoing protection of BSI information assets including client data;

iii. monitor and review the ISMS by regularly assessing the effectiveness of the ISMS, against the Information Security Policy, objectives and plans;

iv. report findings related to the performance of the ISMS to the Information Security Steering Committee and Executive Management for review;

v. maintain and improve the ISMS, based on the results of the internal ISMS audit and the management review process, both of which will identify corrective actions, as well as issues, risks and opportunities;

vi. take into account legal and regulatory requirements, specifically when monitoring and reviewing the ISMS and running the internal compliance programme;

vii. adopt business continuity management practices, to protect critical business processes from unplanned disruptions;

viii. report any actual or suspected breaches of information security to line managers. These will be recorded and investigated by those with responsibility for information security, led by Group Internal Audit and Risk; and

ix. ensure all personnel, suppliers, clients and interested parties (including visitors) are made aware of their information security obligations through communications, contracts, training and policies.

5. Exception Process

The business reasons for considering any exception to this policy must be documented and sent Corporate Compliance Team for approval.

Appendix A – Evaluating Measurable Objectives

Ref	IS Objective	Measure	Tool
1.	Protect the confidentiality, integrity and availability of BSI's information assets	• Monitoring, reviewing and analysing the reported incidents • Monitoring and measuring the number of individuals who have been trained	• Incident Register • Induction webinar on information security and LMS system report
2.	Provide information, with minimal disruption to personnel, suppliers, clients and interested parties, as required by BSI and the appropriate compliance and regulatory framework	• Monitoring and measuring the frequency of Business Continuity disruptions and resolution period • Monitoring and measuring the reported incidents	• BCP Test Reports • Incident Register
3.	Increase client confidence in BSI's ability to protect client information entrusted to it	• Monitoring the compliance with ISO27001 and the number of NCRs	• Issue of 27001 certificate • Non conformities (NCRs)
4.	Protect the reputation of BSI and enhance BSI brand value	• Evaluating the number and severity of incidents affecting external parties	• Incident Register
5.	Reduce the risk of information security breaches, incidents and loss of data and information assets	• Evaluation of risk assessments and reviews and monitoring of the level of the residual risk	• Controls Implemented • Risk Treatment Plan • Third party penetration tests
6.	Comply with data protection laws on the protection of personal data, both as a data controller and as a data processor (see ***Privacy Policy*** for further information)	• Monitoring and evaluation of the number of personal data breaches • Responding to DSARs	• Information Security incident tickets • Technology to facilitate DSARs

7.	Reduce the risk of personal data breaches and protect the rights of data subjects (see ***Privacy Policy*** for further information)	- Number of complaints received by local authority for privacy - Number of communications to local authority for privacy	- Local authority for privacy reports
8.	Increase personnel and supplier awareness to information security threats	- Monitoring the reporting of incidents to personnel and suppliers - Number of regular communications through IS Champions and Reps to personnel and suppliers - Monitoring of induction and annual refresher training and testing	- Incident Register - IS Policies - IS Comms Page - IS Online Webinar - IS Champion and Reps meetings - Interactive Services
9.	Recognise BSI expertise in applying management systems by gaining third party recognition of the ISMS	- Maintenance and extension of ISO27001:2013 certification	- ISO27001:2013 Certificate
10.	Provide a structured approach to securing information, led senior management who are committed to continual improvement of the ISMS	- Monitoring of the Management Review participation - Monitoring and evaluation of the compliance to policy	- Mgt Review record - Internal Audit NCRs

Revision History

Revision No.	Date	Author	Approved By	Changes
01	6 Dec 2011	Lorraine Orr	Howard Kerr	NEW
02	9 Nov 2012	Lorraine Orr	Howard Kerr	Updated to include ref to global compliance
03	10 Sep 2013	Lorraine Orr	Howard Kerr	Removed specific reference to UK and changed classification to public. Added all countries by 2015.
04	5 Sept 014	Lorraine Orr	Howard Kerr	Minor changes to meet 2013 version of ISO27001:2005
05	18 Sep 2014	Lorraine Orr	Howard Kerr	Added table for Measurable objectives
06	13 Sep 2016	Michaela Chiocca	Howard Kerr	Changed Group Risk and Compliance to Group Internal Audit and Risk. Updated Scope, intent and measurable objectives.
07	31 Mar 2017	Michaela Chiocca	Howard Kerr	Changed categories of information assets in Purpose section
08	11 Feb 2019	Massimo Solari	Howard Kerr	Reviewed objectives and organisational details
09	29 May 2020	Massimo Solari	Howard Kerr	Updated
10	02 July 2020	Joanne Leigh, Massimo Solari, Simon White	Howard Kerr	Conformed to master glossary and updated formatting
11	January 2021	Massimo Solari, Simon White	Susan Taylor Martin	Reissued for 2021