BSI Information Security Policy

Table of Contents

1. Purpose

The purpose of the Information Security Policy is to describe the information security objectives of The British Standards Institution ("BSI") for protecting our information assets. This is the primary policy under which all other information security related polices reside. A minimum standard is achieved by following this policy.

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

2. Definitions

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 IT systems.
Information, and related processes, systems, networks and people are also important assets in achieving the information security objectives.
BSI information assets are grouped into the following categories:

- Information, such as data, documents, intellectual property, knowledge, application and system software documentation, not only in electronic media (databases, files in PDF, Word, Excel, and other formats), but also in paper and other forms.
- Hardware including, but not limited to laptops, servers, printers, mobile devices and removable media
- Applications & System Software - not only purchased but also freeware
- Infrastructure, such as offices, electricity supply and air conditioning, because these assets can cause lack of availability of information
- People - often a single point of contact and have information in their head which isnot available in other forms
- Outsourced services, for example legal services or cleaning services, and also onlineservices like Dropbox or Gmail. Whilst these may not be considered assets as per the definition, such services need to be similarly controlled

3. Scope

This policy, together with all supporting controls, processes, and procedures, applies to:

- All BSI personnel, regardless of location. This includes any personnel under the supervision, guidance or management of BSI staff and external parties that provide information processing services to BSI.
- All Information Assets for which BSI has ownership and/or a legal, regulatory, or contractual responsibility.

This policy extends to information assets held by BSI on behalf of third parties and partners, and by

third parties and partners on behalf of BSI.

4. Responsibilities

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.

The Chief Information Security Officer (CISO) is responsible for:

- the implementation and deployment of the ISMS across BSI
- defining, managing and ensuring compliance with the ISMS.

5. 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 asset.

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.

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

6. Intent of the ISMS

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.

BSI commits that it will:

i. Take a risk-based approach to managing information assets in order to minimize 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.

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.

7. Compliance

Policy compliance will be monitored by the Head of Compliance and in accordance with internal governance procedures. Activities related to the policy may be logged and audits of control effectiveness will be undertaken by the Information Security Assurance team, as part of the Information Security Management System (ISMS), and by the Internal Audit team. External audits will be carried out as part of our ISO 27001 certification.

Failure to comply may be treated as a disciplinary matter and addressed in accordance with contracts of employment and HR disciplinary policies.

Appropriate action will be taken in all cases of suspected criminal activity and offences may be reported to the local law enforcement agency or other appropriate authority and could lead to civil or criminal proceedings.

If personnel are in any doubt that an action is not compliant with policies, or need assistance with interpreting or applying these policies, they should seek advice from their line manager or the Information Security team. Alternatively you may also report the incident anonymously by using the Speak Up service, accessible via the following link:

https://www.bsigroup.com/en-GB/about-bsi/ethics-and-compliance

8. Exception Process

Every effort must be made to comply with this policy and all associated policies, procedures and standards. Where it is not possible to apply or enforce any part of a policy, for operational or legitimate business reasons, a policy exemption request should be submitted in accordance with the Policy Exemption Request Process.