Information Security Policy

Your partner
in progress

Table of Contents

1 Purpose

The purpose of this 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, in line with ISO 27001:2022. The framework consists of policies, processes and procedures supported by both management and technical controls appropriate to the risk profile of BSI.

2 Definitions

The terms and definitions used in this policy align to those provided in ISO/ IEC 27000:2020.

Information Asset: is a body of 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. It is defined and managed as a single unit so it can be understood, shared, protected, and utilised efficiently. Information Assets have recognisable and manageable value, risk, content, and lifecycles.

Information, and related processes, systems, networks and people are all important assets in achieving the information security objectives.

BSI information assets may be grouped into the following categories:

- Information: such as data, personal 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 or developed by BSI, 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 is not available in other forms.
- Outsourced Services: for example, legal services or cleaning services, and also online services, such as email and file sharing services. 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, including outsourced services, for which BSI has ownership and/or a legal, regulatory, or contractual obligations.

- Information assets held by BSI on behalf of clients, 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 ISMS framework that underpins it. Managers are responsible for ensuring that this policy is implemented effectively and ensuring compliance within their teams.

Chief Information Security Officer (CISO) is accountable for:

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

5 Information Security Objectives

The following objectives apply across BSI:

1. Protect the confidentiality, integrity and availability of BSI’s, client's and partner's information assets.
2. Provide information, with minimal disruption to personnel, suppliers, clients and interested parties, within the appropriate compliance and regulatory frameworks and policy requirements.
3. Increase clients’ and stakeholders’ confidence in BSI’s ability to protect the information assets entrusted to it.
4. Protect the reputation of BSI and enhance BSI brand value.
5. Reduce the risk of information security and personal data breaches, incidents and loss of data and information assets.
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).
7. To implement effective technical and organisational controls to reduce the likelihood and impact of a data breach or security incident (see Privacy Policy for further information).
8. All personnel and suppliers are made aware of information security, privacy and compliance threats, risks & best practice, and that adequate training is provided to improve awareness and vigilance and to ensure users are competent to carry out their role.
9. Recognise BSI expertise in applying management systems by gaining third party recognition of the ISMS.
10. 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”), chaired by the Chief Information Security Officer (CISO), has been established to oversee the achievement of these objectives.

BSI Leadership is committed to:

a) ensuring that the information security policy and the information security objectives are compatible with the strategic direction of the organization;

b) ensuring that the information security management system (ISMS) requirements are integrated into the organization's processes;

c) ensuring that the resources needed for the ISMS are available, by allocating resources, responsibilities and authority which will be regularly reviewed by Executive Management to ensure the ongoing protection of BSI information assets including client data;

d) communicating the importance of effective information security management and of conforming to the ISMS requirements;

e) ensuring that the ISMS achieves its intended outcomes by regularly assessing its effectiveness against the information security objectives;

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement of the ISMS, based on the results of the internal ISMS audits and the management review processes, which will identify corrective actions, as well as issues, risks and opportunities;

h) taking a risk-based approach to managing information assets in order to minimise the risk of information security incidents and data breaches.

i) taking into account all relevant legal and regulatory obligations, specifically when monitoring and reviewing the effectiveness of the ISMS.

j) adopting business continuity management practices, to protect critical business processes from unplanned disruptions;

k) fostering a culture where the reporting of any actual or suspected breach of information security is actively encouraged and ensuring such incidents are recorded and investigated by those with responsibility for information security and data protection; and

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

7 Policy Compliance

In alignment with our Code of Business Ethics, breaches of this policy can result in remedial, corrective, or disciplinary actions up to and including termination of employment. Actual or suspected incidents of misconduct should be reported to Group Compliance at compliance@bsigroup.com. BSI guarantees non-retaliation and confidentiality, to the extent legally possible, for good-faith reports of such breaches.

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.

BSI has partnered with Safecall to provide an independent externally hosted reporting line “SpeakUp” where you may raise your concerns relating to application or breaches of this policy anonymously. All reports are treated with the utmost confidentiality by independent staff. For further information on raising concerns and access to our Speak Up reporting line, please visit the page below:

https://bsigroup.sharepoint.com/sites/complianceethics/SitePages/Speak-Up.aspx

If personnel are in any doubt that an action is not compliant with this policy, or need assistance with interpreting or applying this policy, they should seek advice from their line manager or from the Information Security team: infosec@bsigroup.com

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 must be submitted in accordance with the Policy Exemption Request Process and approval obtained prior to any deviation from policy.

9 Revision

Revision No	Date	Author	Approved By	Changes
15	June 2024	Global Head of Information Security, Assurance & Compliance	CISO	

Appendix A – Evaluating Measurable Objectives

	Objective	Measures	Tools/ Evidence
1	Protect the confidentiality, integrity and availability of BSI’s, client's and partner's information assets.	Number of high impact information security incidents reported by users	Service Now tickets
		Number of actual phishing attacks reported (clicked link and/or submitted credentials)	Phishing simulations managed by and reported by IS Team
2	Provide information, with minimal disruption to personnel, suppliers, clients and interested parties, within the appropriate compliance and regulatory frameworks and policy requirements.	% of Technology Resilience Tests Completed vs Planned	IT Continuity (DR)/ Resilience Test Plan and Reports
3	Increase clients’ and stakeholders’ confidence in BSI’s ability to protect the information assets entrusted to it.	Number of internal and external audits performed (versus planned)	Entropy - Audit Statistics Report
		% of Findings (NCs & OFIs) overdue	Entropy - monthly reporting
4	Protect the reputation of BSI and enhance BSI brand value	Data Incidents & Breaches (# incidents; low/medium/ high)	Service Now tickets Security HQ Compliance reports
		Maintain the information security, privacy and cybersecurity compliance on 75% of our suppliers	Supplier Due Diligence Dashboard
		% of Suppliers Audit Index on High lees than 10%	Supplier Due Diligence Dashboard
5	Reduce the risk of information security and personal data breaches, incidents and loss of data and information assets.	% of risk registers reviewed and updated in the year vs planned within Metricstream	Metricstream
		Number of high risks identified during the risk assessment within Metricstream	Metricstream

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)	Data subject requests (year to date)	Reports to DPO of potential personal data breaches
		Responding to Data Subject Access Request (DSAR)	Compliance team/ DPO records
7	To implement effective technical and organisational controls to reduce the likelihood and impact of a data breach or security incident.(see Privacy Policy for further information).	Fulfil all data subject requests within the required timeframe	Compliance team/ DPO records
		Notifications to the supervisory Authority in the event of a data breach	Compliance team/ DPO records
8	All personnel and suppliers are made aware of information security, privacy and compliance threats, risks & best practice, and that adequate training is provided to improve awareness and vigilance and to ensure users are competent to carry out their role.	Number of regular communications completed VS planned at the communication plan.	Intranet and targeted comms
		% of employees overdue on completing the mandatory annual information security training	Workday report
		% of contingent workers overdue on completing the mandatory annual information security training	Workday report
		All members of the IS team have undertaken the relevant training to carry out their role	Relevant certifications incl. ISO 27001:2022 Lead Auditor
9	Recognise BSI expertise in applying management systems by gaining third party recognition of the ISMS.	Successful transition to ISO 27001:2022	ISO27001:2022 Certificate
		Maintenance and extension of ISO27001 certification	Audit Schedule
10	Provide a structured approach to securing information, led by senior management who are committed to continual improvement of the ISMS.	Management Review completed Vs Planned	Management Review meeting minutes (GLT, AMAS, APAC)
		Management Review actions completed on time	Management Review meeting minutes (GLT, AMAS, APAC)