



Information Security Policy

Purpose:

The BSA Group of Companies and its Subsidiaries (BSA) are committed to the delivery of products and services in compliance with information security requirements including regulatory, contractual, and internal controls, both for internal activities and for projects controlled by the Company.

BSA's overriding objective is to achieve continual improvement of the management of information security within the organisation. This policy expresses the intent of management with respect to information security within the organisation to safeguard three main objectives for the protection of client information, BSA corporate information, information systems, and end-customer information:

- Confidentiality – data and information assets must be confined to the people authorised to access them and not be disclosed to others.
- Integrity – data must be kept intact, complete, and accurate and systems must be kept operational.
- Availability – the information or system must be available for use by authorised users when required.

This Policy supports and is supported by the Code of Conduct and the BSA Information Security Management System.

Approach:

BSA seeks to achieve this purpose through:

- Fostering a culture that is based on Information Security leadership and effective consultation with key stakeholders, both internal and external, to achieve and improve Information Security standards and performance.
- Our Information Security Management System (ISMS), the documented standards and controls which together describe a multi-layered view of BSA's Information Security strategy, commitment, requirements, and processes.
- Compliance with all relevant Information Security legal and regulatory requirements, the Code of Conduct, Company policies, standards, and procedures.
- Establishing and maintaining those external certifications that support the business.
- Establishing information security objectives and targets and reporting mechanisms to track and measure progress.
- The elimination or, if not reasonably practical, the minimisation of information security risks.
- Identifying, reporting, and investigating information security incidents, non-conformity of standards and controls, and implementing corrective and preventive actions.
- Training of employees in the Information Security standards and the relevant controls and procedures.
- Requiring all workers take reasonable care, complying with all reasonable instructions, with the security of client information, BSA corporate information, information systems, and end-customer information.




- Thorough and timely investigations of reported Information Security incidents, near misses and vulnerabilities through early identification, notification, and methodical investigation.
- Sharing of learnings across the BSA Group of companies and subsidiaries.
- Measuring, monitoring, and auditing the effectiveness of our Information Security Management System using audit and governance and continual improvement processes.

Application:

This Policy applies to all BSA operations, applicable to both BSA employees and contractors, covering all our activities and services. The management teams have the accountability to understand the Policy and bring it to life.

The Policy is owned by the Board and enacted through the Joint Chief Executive Officers. It will be reviewed biennially and/or updated as required due to changes in the business, its leadership, or the environment within which we operate.

Two handwritten signatures in black ink. The first signature is 'Arno Becker' and the second is 'Richard Bartley'.

Arno Becker and Richard Bartley
Joint CEOs – BSA Limited