STRATEGICGROUP
YOUR TRUSTED IT PARTNER

Strategic Group Information Security Management System (ISMS) Policy Statement

Last Revision: 18/08/2023

Document Version: 1.2

Information Security Management (ISMS) System Policy Statement

Strategic Group is committed to implementing an Information Security Management System (ISMS) to ensure information systems are appropriately protected from loss of confidentiality, integrity, and availability.

This document provides an overview of requirements of Strategic Group management and employees regarding information security. It identifies the requirements for an effective information security management system, sets objectives and provides the overall view of management regarding information security.

Our commitment is to ensure that Strategic Group:

- Implement and maintain an effective and auditable Information Security Management System.
- Maintain appropriate systems to ensure integrity and protection against unauthorised alteration or destruction.
- Employees and users of Strategic Group systems have timely and reliable access to information and services.
- Promote security of information and information systems.
- Employees understand the importance of information security and comply with all policy, procedures and standards regarding information and information assets.
- Aligns risk assessment practices relating to the ISMS with Strategic Group's Risk Management Framework.
- Implement controls for identified risks, threats and vulnerabilities.
- Set a baseline for information security and continue to improve the management system.
- Complies with statutory, legislative and government direction regarding information security.
- Provide assurance to our business network that information held is appropriately protected and handled.

The following principles underpin this policy statement:

- Alignment and compliance with requirements of the ISO/IEC 27001:2013 Information Security Management standard.
- Annual attestation of compliance to ISO/IEC 27001:2013

Strategic Group ISO:27001 Statement of Applicability

This document provides an overview of the scope and controls that are applicable to Strategic Groups' certification of ISO:27001/2013 and make up the Information Security Management System (ISMS) which is maintained and audited regularly in accordance to the standard.

Standard: ISO 27001:2013 Information Security Management System Requirements

Scope: Strategic Group are an Australian IT Managed Services company that provide a wide range of IT services to SME's across Australia including private cloud, on-site servers, IT managed services and professional services in accordance with this Statement of Applicability.

AREA/SECTION	APPLICABILITY
A.5 Information security policies	
A.5.1.1 Policies for information security	Yes
A.5.1.2 Review of the policies for information security	Yes
A.6 Organization of information security	
A.6.1.1 Information security roles and responsibilities	Yes
A.6.1.2 Segregation of duties	Yes
A.6.1.3 Contact with authorities	Yes
A.6.1.4 Contact with special interest groups	Yes
A.6.1.5 Information security in project management	Yes
A.6.2.1 Mobile device policy	Yes
A.6.2.2 Teleworking	Yes
A.7 Human resources security	
A.7.1.1 Screening	Yes
A.7.1.2 Terms and conditions of employment	Yes
A.7.2.1 Management responsibilities	Yes
A.7.2.2 Information security awareness, education and training	Yes
A.7.2.3 Disciplinary process	Yes
A.7.3.1 Termination or change of employment responsibilities	Yes
A.8 Asset Management	
A.8.1.1 Inventory of assets	Yes
A.8.1.2 Ownership of assets	Yes
A.8.1.3 Acceptable use of assets	Yes
A.8.1.4 Return of assets	Yes
A.8.2.1 Classification of information	Yes
A.8.2.2 Labelling of information	Yes
A.8.2.3 Handling of assets	Yes
A.8.3.1 Management of removable media	Yes
A.8.3.2 Disposal of media	Yes
A.8.3.3 Physical media transfer	Yes
A.9 Access control	
A.9.1.1 Access control policy	Yes
A.9.1.2 Access to networks and network services	Yes
A.9.2.1 User registration and de-registration	Yes
A.9.2.2 User access provisioning	Yes
A.9.2.3 Management of privileged access rights	Yes
A.9.2.4 Management of secret authentication information of users	Yes

A.9.2.5 Review of user access rights	Yes
A.9.2.6 Removal or adjustment of access rights	Yes
A.9.3.1 Use of secret authentication information	Yes
A.9.4.1 Information access restriction	Yes
A.9.4.2 Secure log-on procedures	Yes
A.9.4.3 Password management system	Yes
A.9.4.4 Use of privileged utility programs	Yes
A.9.4.5 Access control to program source code	No
A.10 Cryptography	
A.10.1.1 Policy on the use of cryptographic controls	Yes
A.10.1.2 Key management	Yes
A.11 Physical and environment security	
A.11.1.1 Physical security perimeter	No
A.11.1.2 Physical entry controls	Yes
A.11.1.3 Securing offices, rooms and facilities	Yes
A.11.1.4 Protecting against external and environmental threats	No
A.11.1.5 Working in secure areas	No
A.11.1.6 Delivery and loading areas	No
A.11.2.1 Equipment siting and protection	Yes
A.11.2.2 Supporting utilities	Yes
A.11.2.3 Cabling security	Yes
A.11.2.4 Equipment maintenance	Yes
A.11.2.5 Removal of assets	Yes
A.11.2.6 Security of equipment and assets off-premises	Yes
A.11.2.7 Secure disposal or reuse of equipment	Yes
A.11.2.8 Unattended user equipment	Yes
A.11.2.9 Clear desk and clear screen policy	Yes
A.12 Operations security	
A.12.1.1 Documented operating procedures	Yes
A.12.1.2 Change management	Yes
A.12.1.3 Capacity management	Yes
A.12.1.4 Separation of development, testing and operational environments	No
A.12.2.1 Controls against malware	Yes
A.12.3.1 Information backup	Yes
A.12.4.1 Event logging	Yes
A.12.4.2 Protection of log information	Yes
A.12.4.3 Administrator and operator logs	Yes
A.12.4.4 Clock synchronisation	Yes
A.12.5.1 Installation of software on operational systems	Yes
A.12.6.1 Management of technical vulnerabilities	Yes
A.12.6.2 Restrictions on software installation	Yes
A.12.7.1 Information systems audit controls	Yes
A.13 Communications security	
A.13.1.1 Network controls	Yes
A.13.1.2 Security of network services	Yes
A.13.1.3 Segregation in networks	Yes

A.13.2.1 Information transfer policies and procedures	Yes
A.13.2.2 Agreements on information transfer	Yes
A.13.2.3 Electronic messaging	Yes
A.13.2.4 Confidentiality or nondisclosure agreements	Yes
A.14 System acquisition, development and maintenance	
A.14.1.1 Information security requirements analysis and specification	Yes
A.14.1.2 Securing application services on public networks	Yes
A.14.1.3 Protecting application services transactions	Yes
A.14.2.1 Secure development policy	No
A.14.2.2 System change control procedures	No
A.14.2.3 Technical review of applications after operating platform changes	No
A.14.2.4 Restrictions on changes to software packages	No
A.14.2.5 Secure system engineering principles	No
A.14.2.6 Secure development environment	No
A.14.2.7 Outsourced development	No
A.14.2.8 System security testing	No
A.14.2.9 System acceptance testing	No
A.14.3.1 Protection of test data	No
A.15 Supplier relationships	
A.15.1.1 Information security policy for supplier relationships	Yes
A.15.1.2 Addressing security within supplier agreements	Yes
A.15.1.3 Information and communication technology supply chain	Yes
A.15.2.1 Monitoring and review of supplier services	Yes
A.15.2.2 Managing changes to supplier services	Yes
A.16 Information security incident management	
A.16.1.1 Responsibilities and procedures	Yes
A.16.1.2 Reporting information security events	Yes
A.16.1.3 Reporting information security weaknesses	Yes
A.16.1.4 Assessment of and decision on information security events	Yes
A.16.1.5 Response to information security incidents	Yes
A.16.1.6 Learning from information security incidents	Yes
A.16.1.7 Collection of evidence	Yes
A.17 Information security aspects of business continuity management	
A.17.1.1 Planning information security continuity	Yes
A.17.1.2 Implementing information security continuity	Yes
A.17.1.3 Verify, review and evaluate information security continuity	Yes
A.17.2.1 Availability of information processing facilities	Yes
A.18 Compliance	
A.18.1.1 Identification of applicable legislation and contractual requirements	Yes
A.18.1.2 Intellectual property rights	Yes
A.18.1.3 Protection of records	Yes
A.18.1.4 Privacy and protection of personally identifiable information	Yes
A.18.1.5 Regulation of cryptographic controls	No
A.18.2.1 Independent review of information security	Yes
A.18.2.2 Compliance with security policies and standards	Yes
A.18.2.3 Technical compliance review	Yes

Strategic Group ISO:27017 Statement of Applicability

This document provides an overview of the scope and controls that are applicable to Strategic Groups' certification of ISO 27017:2015 and make up the Information Security Management System (ISMS) which is maintained and audited regularly in accordance to the standard.

Standard: ISO 27017:2015 – Information Technology - Cloud

Scope: Strategic Group are an Australian IT Managed Services company that provide a wide range of IT services to SME's across Australia including private cloud, on-site servers, IT managed services and professional services in accordance with this Statement of Applicability.

AREA/SECTION	APPLICABILITY
A.5 Information security policies	
A.5.1.1 Policies for information security	Yes
A.5.1.2 Review of the policies for information security	Yes
A.6 Organization of information security	
A.6.1.1 Information security roles and responsibilities	Yes
A.6.1.3 Contact with authorities	Yes
CLD.6.1.3 Shared roles and responsibilities within a cloud computing environment	Yes
A.7 Human resources security	
A.7.2.2 Information security awareness, education and training	Yes
A.8 Asset Management	
A.8.1.1 Inventory of assets	Yes
CLD.8.1.5 Removal of cloud service customer assets	Yes
A.8.2.2 Labelling of information	Yes
A.9 Access control	
A.9.1.2 Access to networks and network services	Yes
A.9.2.3 Management of privileged access rights	Yes
A.9.2.4 Management of secret authentication information of users	Yes
A.9.4.1 Information access restriction	Yes
A.9.4.4 Use of privileged utility programs	Yes
CLD.9.5.2 Virtual machine hardening	Yes
A.10 Cryptography	
A.10.1.1 Policy on the use of cryptographic controls	Yes
A.10.1.2 Key management	Yes
A.11 Physical and environment security	
A.11.2.7 Secure disposal or reuse of equipment	Yes
A.12 Operations security	
A.12.1.2 Change management	Yes
A.12.1.3 Capacity management	Yes
CLD.12.1.5 Administrator's operational security	Yes
A.12.3.1 Information backup	Yes
A.12.4.1 Event logging	Yes
A.12.4.2 Protection of log information	Yes
A.12.4.3 Administrator and operator logs	Yes
A.12.4.4 Clock synchronisation	Yes
CLD.12.4.5 Monitoring of cloud services	Yes
A.12.6.1 Management of technical vulnerabilities	Yes

A.13 Communications security	
A.13.1.3 Segregation in networks	Yes
A.14 System acquisition, development and maintenance	
A.14.1.1 Information security requirements analysis and specification	Yes
A.14.2.1 Secure development policy	No
A.15 Supplier relationships	
A.15.1.1 Information security policy for supplier relationships	Yes
A.15.1.2 Addressing security within supplier agreements	Yes
A.16 Information security incident management	
A.16.1.1 Responsibilities and procedures	Yes
A.16.1.2 Reporting information security events	Yes
A.16.1.7 Collection of evidence	Yes
A.18 Compliance	
A.18.1.1 Identification of applicable legislation and contractual requirements	Yes
A.18.1.2 Intellectual property rights	Yes
A.18.1.3 Protection of records	Yes
A.18.1.5 Regulation of cryptographic controls	Yes
A.18.2.1 Independent review of information security	Yes

Name	Position	Signature	Date
Chris Boswell	CEO	Chris Boswell	18/08/2023