Everest engineering

Information security policy

ISM.01

Version 0.2.3

July 1 2025

Contents

1 Introduction

Sound technical choices, a culture of personal and shared responsibility and accountability, and risk management are essential to promoting an organisation wide security mindset. This document describes the security policy that applies at Everest Engineering to protect ourselves, our customers and third party individuals who have an interest in what and how we conduct our business.

Implementation of this policy is delegated to relevant organisation-wide or localised procedures where applicable.

Customers may have specific security requirements that differ from our policies. This may require you to understand and comply with customer security requirements and to adjust your work practices and tooling as appropriate. Whether this applies depends on the type of the engagement and the maturity of our customer.

1.1 Policy responsibility

All members of Everest Engineering hold delegated responsibilities as defined in ISM.02: *Roles and responsibilities*.

1.2 Contacting us

Speak up if something concerns you!

It is important that we address weaknesses in our internal systems and in the projects that we contribute to. Please submit feedback and concerns by emailing `security@everest.engineering`.

You can also discuss general security topics in the `#security` channel on Slack.

Refer to ISM.103: *Incidence management procedure* in case of a known or suspected security incident.

1.3 Policy status

This policy is open to continual improvement, both through formal review processes and through feedback from its stakeholders. This includes: the leadership team, Everest Engineering employees, our customers and our investors. It will also be formally reviewed every six months to ensure it continues to satisfy our information security requirements.

This policy is endorsed by the Everest Engineering leadership team.

The next review of this policy is due 15 February 2025.

1.4 Objective setting

Security objectives are set through monthly security sprint reviews held between the Everest Engineering leadership team and the security team. Current and backlog objectives are discussed and prioritised based on the current and emerging needs of the business.

Records of meetings are documented on our internal Notion page. Formal changes such as the adoption of new security controls that result from these reviews will be captured as part of the change management processes in our information security practices repository.

1.5 Appropriateness and continual improvement

Our security policy is tailored to meet the needs of the organisation based on the documented organisational context and the derived information security management system (ISMS) scope. This is reviewed annually and cascaded down to policy.

As well as incorporating improvements arising from monthly security sprint reviews, feedback from employees, customers, suppliers and outside risk assessment reports will also be considered.

The security team maintains a risk register and is responsible for incorporating feedback in the register.

2 Information security organisation

2.1 Internal organisation

These controls guide internal organisational roles, the cascade of responsibilities and segregation of duties.

2.1.1 Roles and responsibilities

Control: information security responsibilities will be defined and allocated.

Individuals mapped to a security role are responsible for the protection of the assets (both information and devices) under their control and for ensuring that security processes are enforced.

Refer to ISM.02: *Roles and responsibilities*.

2.1.2 Segregation of duties

Control: conflicting duties and areas of responsibility will be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of assets.

2.1.3 Contact with authorities

Control: appropriate contacts with relevant authorities will be maintained.

The security team will maintain a list of relevant authorities, under what circumstances they are to be contacted and who is permitted to engage with them.

2.1.4 Contact with special interest groups (SIGs)

Control: contact with appropriate special associations will be maintained.

The aim of this control is to gain access to specialist security information, alerts on current and emerging threats, and a support network of specialists.

2.1.5 Internal project management

Control: information security will be addressed in the management of all projects that affect the security posture of the organisation.

Note that this control is not concerned with projects that we deliver for our customers. Such projects are considered business-as-usual (BAU).

An organisation-wide security mindset requires that information security:

- objectives are included in project objectives;
- risk assessment is conducted at an early stage of the project to identify necessary controls; and
- is part of all phases of the applied project methodology.

2.2 Mobile devices and remote working

Controls for enhancing the security of remote working and mobile devices.

2.2.1 Mobile device policy

Control: appropriate policy will be developed and implemented to manage risks introduced by the use of mobile devices.

Refer to ISM.03: *Mobile device policy*.

2.2.2 Remote working

Control: appropriate policy must be developed and implemented to protect information and devices assets stored at remote working sites.

Refer to ISM.03: *Mobile device policy*.

3 Employees and contractors

3.1 Prior to employment

Controls to ensure employees and contractors understand their responsibilities, are suitable for their considered roles and their private information is protected.

3.1.1 Screening

Control: background screen and verification must be performed on all candidates proportional to the security classification of the information they are required to access in order to perform their duties.

3.1.2 Terms and conditions of employment

Control: contractual agreements with employees and contractors must state their and the organisation's responsibilities for information security.

Refer to ISM.02: *Roles and responsibilities* and ISM.09: *Acceptable use policy*.

3.2 During employment

3.2.1 Management responsibilities

Control: management will require all employees to apply information security in accordance with policy.

Management will cascade information to their reports, ensuring briefings are held, guidance is provided and security awareness is promoted according to the roles and responsibilities of the people in the organisation.

3.2.2 Security awareness training

Control: all employees must undertake regular periodic security awareness training appropriate to their role and responsibilities.

3.2.3 Disciplinary process

Control: a communicated formal disciplinary process must be in place to take action against serious and wilful breach of information security.

3.3 Change of responsibilities or termination

Control: information security responsibilities must remain in place on change of role or on termination of employment, communicated to employees and contractually enforced.

4 Asset management

4.1 Responsibility for assets

Asset management is concerned with identifying and tracking information assets, and the devices used to store and process them in order to apply adequate protection.

4.1.1 Inventory

Control: information and device assets will be identified and tracked.

Security role allocations and asset ownership will assign responsibilities for managing and tracking the lifecycle of assets according to their data classification.

4.1.2 Ownership

Control: information and device assets tracked in the asset register will be owned.

All assets are required to have an assigned owner who has responsibility for the asset. Asset owners must:

- keep the asset up to date in the register;
- classify it according to the data classification scheme;
- periodically review access restrictions and classification, and apply access control policies; and
- ensure the asset is properly deleted or destroyed when retired.

Note that ownership is defined as custodianship and does not imply property rights.

4.1.3 Acceptable use

Control: rules for acceptable use of information and device assets will be identified, documented and implemented.

Refer to ISM.09: *Acceptable use policy*.

4.1.4 Return of assets

Control: all employees and third party users must return all information and device assets upon termination of their employment, contract or agreement.

This extends to information and device assets loaned to us by our customers.

Information assets, once transferred to their owning organisation, must be securely deleted from any device that is owned by an employee or third party.

4.2 Security classification

Appropriate levels of protection must be given to information assets and the devices on which we store and process them.

4.2.1 Classification scheme

Control: information and device assets will be classified according to legal requirements, value, criticality and sensitivity to disclosure or modification.

Refer to ISM.10: *Data classification scheme*.

4.2.2 Classification labelling

Control: appropriate procedures for security classification labelling must be developed and implemented in accordance with our adopted data classification scheme.

Refer to ISM.10: *Data classification scheme*.

4.2.3 Handling of security classified assets

Control: procedures for handling information and device assets must be developed and implemented in accordance with our adopted data classification scheme.

Refer to ISM.10: *Data classification scheme*.

4.3 Media handling

Media must be handled in such a manner as to prevent unauthorised disclosure, modification, removal or destruction of stored information assets.

4.3.1 Removable media

Control: procedures will be implemented to manage removable media in accordance with our adopted data classification scheme.

4.3.2 Disposal

Control: when no longer required, media will be securely disposed of using formal procedures.

A record of the secure disposal must be documented in the asset register.

4.3.3 Physical media transfer

Control: media containing information assets must be protected against unauthorised access, misuse or corruption during transportation.

5 Access control

5.1 Business requirements

Access to information and information processing facilities should be limited.

5.1.1 Access control policy

Control: access control policy will be established and periodically reviewed based on business and information security needs.

This refers to both logical and physical controls.

Refer to ISM.04: *Access control policy*.

5.1.2 Network and network service access

Control: users will only be provided with access to the network and network services that they have been explicitly authorised to use.

Refer to ISM.07: *Network security policy*.

5.2 User access management

Assignment of access rights to limit information access to authorised users and to prevent unauthorised use.

5.2.1 User registration and de-registration

Control: a formal user registration and de-registration process must be implemented to enable appropriate assignment of access rights.

All users must be assigned unique identifiers that associates actions with individuals. Shared accounts are not permitted unless required for exceptional purposes. Such exceptions must be documented, approved and periodically reviewed.

Periodic review of access rights is required.

5.2.2 User access provisioning

Control: a formal user access provisioning process must be implemented to assign or revoke access rights. This must apply to all users and all systems.

This control guides the assignment of access rights and, depending on situation, may require permission from the asset owner to assign access rights. Granting of access rights must be centrally documented for audit purposes. Principles of least privilege must apply, including to users in senior management roles.

Access revocation must be immediate for users that have left the organisation.

5.2.3 Privileged access rights management

Control: assignment and use of privileged access rights must be restricted and controlled.

5.2.4 User credentials management

Control: the allocation of user credentials must be controlled through a formal process.

This includes sharing of temporary credentials and forcing them to be changed on first use, having the user attest that they will not share their individual credentials, the verification of user identities prior to issuing new credentials and sharing credentials over a secure medium.

5.2.5 Review of access rights

Control: asset owners will regularly review users' access rights.

Regularly, here, refers to periodic checks and to events that might trigger a change in access needs. This would include promotions, demotions, termination or moving to a different role.

5.2.6 Removal or adjustment of access rights

Control: access rights of all employees, external parties to information, devices and facilities will be removed or adjusted on their termination of employment, contract or agreement.

The immediacy of the removal or adjustment needs to be evaluated based on which side is initiating the cessation of agreement, their current responsibilities and the value of the assets they are able to access.

5.3 User responsibilities

Individual users are responsible for protecting their personal credentials.

Control: users must adhere to the following Everest Engineering credential practices and procedures:

Refer to ISM.04: *Access control policy*.

5.4 System and application access control

Preventing unauthorised access to systems and applications.

5.4.1 Information access restriction

Control: access to information and application functions must be restricted according to our access control policy.

Refer to ISM.04: *Access control policy*.

5.4.2 Secure login procedures

Control: access to systems and applications must be controlled by secure login procedures.

Secure login procedures: prevent brute force attacks, are not vulnerable to user enumeration attacks, log all successful and unsuccessful logins, encrypt passwords while in transit, store passwords in a secure manner, not mirror passwords back to users as they are being entered.

Highly sensitive systems may be required to terminate inactive sessions and to restrict logins to specific working hours.

5.4.3 Password management systems

Control: password management systems must be interactive and ensure quality passwords.

In addition to enforcing secure login procedures (Section 5.4.2), identity and login implementations must: enforce temporary passwords to be changed on first login, enforce password rotation, enforce secure password selection, and prevent previous passwords from being reused.

5.4.4 Source code access control

Control: access to proprietary source code must be restricted.

6 Cryptography

Cryptographic techniques to protect information in transit and at rest.

6.1 Cryptographic policy

Control: algorithms, including ciphers and hash functions, that comprise encryption techniques must follow the recommendations of NIST SP-800-57.

NIST special publication 800-57 provides guidance and references to more specific NIST publications on acceptable cryptographic algorithms and key material handling.

6.2 Key management

Control: cryptographic keys, their protection and lifetime must follow the recommendations of NIST SP-800-57.

NIST special publication 800-57 provides guidance and references to more specific NIST publications on key management systems.

7 Physical security

For more information on these controls refer to ISM.05: *Physical security policy*.

7.1 Secure areas

The prevention of unauthorised physical access, damage or interference of organisational information assets and processing facilities.

7.1.1 Physical security perimeter

Control: security perimeters must be defined and used to protect areas containing sensitive or critical information and device assets.

7.1.2 Physical entry controls

Control: secure areas must be protected by appropriate entry controls to prevent unauthorised access.

7.1.3 Securing offices, rooms and facilities

Control: appropriate physical security must be defined and implemented for offices, rooms and facilities.

7.1.4 Protection against external and environmental threats

Control: appropriate physical protection must be defined and implemented against natural disasters, malicious attackers and accidents.

7.1.5 Working in secure areas

Control: appropriate procedures must be designed and implemented for working in secure areas.

7.1.6 Delivery and loading areas

Control: access points used for delivery and loading areas, and other points of entry for unauthorised person should be controlled and isolated from information processing facilities as appropriate.

7.2 Equipment security

The securing of equipment to protect stored information and device assets.

7.2.1 Protection of equipment

Control: equipment must be protected against environmental threats, hazards, and unauthorised access.

7.2.2 Supporting utilities

Control: equipment must be appropriately protected against power failures and other utility disruptions.

7.2.3 Cabling security

Control: power and network cabling must be appropriately protected against interception, interference and damage.

7.2.4 Equipment maintenance

Control: equipment must be maintained to ensure availability and integrity.

7.2.5 Asset removal

Control: information and device assets must not be taken off-site without authorisation.

7.2.6 Off-site asset security

Control: appropriate protection must be applied to off-site information and device assets.

7.2.7 Disposal and re-use of equipment

Control: all sensitive information assets and licensed software stored on devices with storage media must be securely removed or destroyed prior to disposal or reuse.

7.2.8 Unattended user equipment

Control: users must ensure that their equipment is appropriately protected when left unattended.

7.2.9 Clear desk and clear screen policy

Control: appropriate clear desk and clear screen policy must be developed and implemented.

8 Operations

8.1 Operational procedures and responsibilities

Authorised, correct and secure operation of information processing facilities.

8.1.1 Documented operating procedures

Control: operating procedures must be documented and made available to operations users.

Documentation should include:

- provisioning and installation of the system;
- automated and manual processing and handling of information;
- backups;
- dependencies between systems;
- procedures for handling errors while performing operational tasks;
- contact information for support staff in case of required escalation;
- system restart and recovery procedures;
- audit trail and log management; and
- operational monitoring concerns.

8.1.2 Change management

Control: changes to the organisation, its processes, its information processing facilities and security systems must be controlled.

The level of formality appropriate to a given system will depend on its sensitivity and criticality. Change management should, however, at a minimum:

- be auditable; and
- be linked to an appropriate business justification.

8.1.3 Capacity management

Control: resource usage must be monitored and projected against future capacity requirements to ensure that usage demands can be met without affecting performance.

8.1.4 Development, test and production environment separation

Control: development, test and production environments must be separated to reduce the risk of unauthorised access or change.

8.2 Malware protection

Control: education and automated controls to detect, prevent and recover from malware must be implemented.

Refer to ISM.06: *Anti-malware policy*.

8.2.1 Backups

Control: backups of information assets and software must be created and regularly rested according to backup policy.

Refer to ISM.13: *Backup policy*.

8.3 Logging and monitoring

8.3.1 Event logging

Control: event logs recording user activities, exceptions, faults and security events must be produced, kept and regularly reviewed.

8.3.2 Log protection

Control: logging facilities and log information must be protected against tampering and unauthorised access.

8.3.3 Clock synchronisation

Control: system clocks of all systems within an organisation or security domain must be synchronised against a single reference time source.

8.4 Installation of software on operational systems

Control: appropriate procedures must be developed and implemented to control the installation of software on operational systems.

8.5 Technical vulnerabilities

8.5.1 Management of vulnerabilities

Control: information about technical vulnerabilities must be obtained and evaluated to determine the risk to the organisation and appropriate measures taken to address risk.

Minimum patching time frames for installation of security patches are as follows:

- **Operating systems of workstations & laptops:** Within one month. Within 48 hours if identified as critical by vendors or working exploits exist.
- **Commonly-targeted applications such as web browsers, and extensions, Office suites, email clients):** Within two weeks. Within 48 hours or as soon as practical if identified as critical by vendors or working exploits exist.
- **Other applications:** Within one month. However, within 48 hours or as soon as practical if identified as critical by vendors or working exploits exist.
- **Operating systems of internet-facing servers:** Within two weeks, or within 48 hours if identified as critical by vendors or working exploits exist

Vulnerability management plans are informed by Australian ASD Essential Eight recommendations, Patching applications and operating systems

Refer to;

- ISM.03: *Mobile device policy*;
- ISM.17: *Software use policy*; and
- ISM.07: *Network security policy*.

8.5.2 Software installation restrictions

Control: appropriate rules must be developed and implemented governing the installation of software by users.

8.6 Audit controls

Control: appropriate audit requirements and activities must be developed and implemented to minimise disruption to business processes.

9 Communications security

9.1 Network security management

Controls protecting networked processing facilities and their information assets.

9.1.1 Network controls

Control: networks must be managed and controlled to protect information assets, systems and applications.

Refer to ISM.07: *Network security policy*.

9.1.2 Network services

Control: security mechanisms, service levels and management requirements must be identified for all network services and included in service agreements.

Refer to ISM.07: *Network security policy*.

9.1.3 Network segregation

Control: logical groups of information services and users must be segregated on networks.

Refer to ISM.07: *Network security policy*.

9.2 Information transfer

Controls protecting information assets transferred internally and between third parties.

9.2.1 Transfer policies and procedures

Control: appropriate policies, procedures and controls must be developed and implemented to protect information assets being transferred through networks and communication facilities.

Refer to:

- ISM.08: *Electronic messaging policy*;
- ISM.09: *Acceptable use policy*;
- ISM.11: *Social media policy*; and
- ISM.12: *Personal information protection*.

9.2.2 Agreements on information transfer

Control: agreements must be in place to protect information asset transfers between organisations.

9.2.3 Electronic messaging

Control: appropriate policies must be developed and implemented to protect information in electronic messaging.

Refer to ISM.08: *Electronic messaging policy*.

9.2.4 Confidentiality and non-disclosure agreements

Control: confidentiality and non-disclosure requirements must be identified, documented and regularly reviewed.

10 System acquisition, development and maintenance

10.1 Information systems security requirements

Controls ensuring that information security is an organisation wide concern and integrated in the entire system lifecycle.

10.1.1 Requirements analysis and specification

Control: security related requirements will be included in the requirements for new information systems or enhancements to existing information processing facilities.

Requirements may be obtained from regulatory compliance requirements, threat modelling, post-incident reviews and vulnerability thresholds. The criticality, value and sensitivity of the information assets should guide requirements.

Requirements management should be incorporated early in the project lifecycle.

Things to consider:

- confidence requirement of claimed user identities for authentication purposes;
- access provisioning and authorisation processes for standard, privileged and administrative users;
- the need to inform users of their responsibilities;
- required protection of the CIA triad (confidentiality, integrity and availability);
- business requirements such as transaction logging, monitoring and non-repudiation; and
- security requirements such as external logging facilities, automated log analysis and attack detection systems.

Supplier contracts should include security requirements when acquiring a product. Product evaluation should include assessing any introduced risk and required mitigations.

10.1.2 Application services on public networks

Control: application service information assets passing over public networks must be protected from fraud, contract disputes, unauthorised disclosure, and unauthorised modification.

In addition to the guidelines enumerated in Section 10.1.1, this control is concerned with the transactional nature of public services. Things to consider:

- informing parties of their authorisation to use a service;
- processes for authorising content of documents, their issuance and signing;
- proof of message dispatch and receipt;
- confidentiality and integrity of transactions, payments and delivery addresses;
- payment verification and fraud prevention;
- liability of fraud; and
- required insurance policies.

10.1.3 Protection of information service transactions

Control: messages involved in service transactions must be protected against incomplete transmission, misrouting, unauthorised alteration, unauthorised disclosure, duplication and replay.

10.2 Development and support processes

Controls promoting the inclusion of information security in system design and implementation.

10.2.1 Secure development policy

Control: appropriate controls for the secure development of software and systems must be established and applied to software and systems developed within the organisation.

This control is concerned with:

- the security of the environment used for development;
- security in the software development lifecycle;
- secure coding standards for the chosen technical stack;
- including security in software and system design;
- incorporating security checkpoints in project delivery;
- securing code repositories against malicious modification and information disclosure;
- version control security;
- application security know-how; and
- the capability of developers to prevent, find and fix technical vulnerabilities.

10.2.2 Change control policies

Control: appropriate change control procedures will be developed and implemented to control changes to systems and software.

The level of formality will depend on the criticality of systems and software, and the sensitivity to disclosure or modification. Generally, all software changes should trace back to a business need with authorisation from the asset owner. Changes should go through an appropriate level of review, either manual or automated, according to the criticality and sensitivity of the production system.

10.2.3 Application technical review following operating platform changes

Control: business critical applications must be reviewed and tested to prevent adverse impact to organisational operation and security following changes to operating platforms.

10.2.4 Software package change restrictions

Control: vendor supplied software package modification should be avoided and must be limited to necessary changes with all changes strictly controlled.

10.2.5 Secure system engineering principles

Control: appropriate principles for secure system engineering must be established, documented, maintained and applied to all information system implementation efforts.

This control is concerned with the people, processes and technology associated with development and integration.

10.2.6 Secure development environment

Control: secure development environments covering the entire SDLC must be established for system development and integration.

10.2.7 Outsourced development

Control: outsourced system development must be supervised and monitored.

This control relates to software that is developed by an outsourced party and includes open source software not internally developed.

Things to consider:

- licensing, code ownership and patents of outsourced content;
- requirements for secure design, coding and testing;
- acceptance testing, quality and accuracy;
- evidence of security thresholds being used to establish minimum security and privacy quality;
- evidence of testing to guard against intentional and unintentional malicious content;
- evidence of testing for known vulnerabilities;
- escrow arrangements to ensure code availability;
- the right to audit development processes and controls; and
- quality of build environment documentation.

10.2.8 Systems security testing

Control: system security functionality must be tested during development.

10.2.9 System acceptance testing

Control: appropriate system acceptance criteria and testing must be established for new information systems and modifications.

10.3 Test data

The protection of data used for test purposes.

10.3.1 Protection

Control: data used for testing must be protected and controlled.

Ideally, data used for testing should be desensitised. If not:

- production access controls should apply equally to test systems;
- egress of production data to a test environment should be separately authorised and controlled;
- production data should be erased from the test environment following test completion; and
- copying of production data should be logged to create an audit trail.

11 Supplier management

11.1 Supplier relationships

Controls to protect organisational information assets accessible by third party suppliers.

11.1.1 Supplier relationship information security policy

Control: requirements to mitigate risks associated with supplier access to organisational information assets will be agreed with suppliers and documented.

Such requirements may include all requirements mentioned in this security policy document.

11.1.2 Addressing security within supplier agreements

Control: information security requirements will be established and agreed with each supplier that will access, process, store, communicate, or provide infrastructure for, organisational information assets.

11.1.3 ICT supply chain

Control: agreements with suppliers will include requirements to address risks associated with ICT services and product supply chains.

11.2 Supplier service delivery management

11.2.1 Supplier services review and monitoring

Control: organisations must regularly review and audit supplier service delivery.

11.2.2 Supplier service change management

Control: changes to supplier service provisioning such as maintaining and improving information security policies, procedures and controls will take into account the criticality of organisational information and device assets, processes and reassessment of risk.

12 Incident management

12.1 Managing information security incidents

Controls to identify and respond to security incidents.

12.1.1 Responsibilities and procedures

Control: responsibilities and procedures will be developed and implemented to ensure rapid response to information security incidents.

Refer to ISM.103: *Incident management procedures*.

12.1.2 Event reporting

Control: information security events will be reported through management channels as soon as possible.

Refer to ISM.103: *Incident management procedures*.

12.1.3 Vulnerability reporting

Control: employees and contractors must report all observed or suspected security weaknesses.

Refer to ISM.103: *Incident management procedures*.

12.1.4 Handling of information security events

Control: information security events will be assessed to determine whether they should be classified as information security incidents.

12.1.5 Handling of information security incidents

Control: information security incidents must be handled according to documented procedures.

Refer to ISM.103: *Incident management procedures*.

12.1.6 Learning from information security incidents

Control: learning by analysing and resolving security incidents should be used to reduce the likelihood and impact of future incidents.

Refer to ISM.103: *Incident management procedures*.

12.1.7 Evidence collection

Control: appropriate procedures will be developed and implemented to identify, collect, and acquire information related to a security incident in order to preserve it as evidence.

Refer to ISM.103: *Incident management procedures*.

13 Business continuity management

13.1 Information security continuity

Controls to protect against major incidents such as crisis and disaster.

13.1.1 Planning

Control: requirements for continuity of information security management will be developed for adverse situations.

13.1.2 Implementation

Control: processes, procedures and controls will be developed, documented and implemented to maintain information security continuity during an adverse situation.

13.1.3 Review

Control: information security continuity requirements and implemented controls will be regularly reviewed.

13.2 Redundancy

13.2.1 Information processing facilities

Control: information processing facilities will be implemented with redundancy to meet business requirements.

14 Compliance

14.1 Legal compliance

Controls to avoid breaches of law and contractual agreements.

14.1.1 Compliance with legislation and contractual requirements

Control: legislation, regulations and contractual obligations will be identified and tracked with documented approaches to meeting these requirements.

14.1.2 Copyright and licensing

Control: appropriate procedures will be developed and implemented to ensure copyright law and licensing agreements are complied with.

14.1.3 Record retention

Control: records will be protected against loss, destruction, unauthorised modification, and unauthorised release as required by law, contractual agreements and business requirements.

Refer to:

- ISM.12: *Personal information protection*;
- ISM.15: *Privacy policy*.

14.1.4 Protection of personally identifiable information

Control: collection, use, disclosure, storage, and disposal of personally identifiable information (PII) will be protected in accordance with the Privacy Act 1988 (Cth) and other relevant legislation.

Refer to:

- ISM.12: *Personal information protection*;
- ISM.15: *Privacy policy*.

14.2 AI Policy

14.2.1 Responsible Use of AI

Control: Employees must use AI technology responsibly and ethically, avoiding any actions that could harm others, violate privacy, or facilitate malicious activities.

Refer to ISM.16: *AI Policy*.

14.2.2 Compliance with laws and regulations

Control: AI technology must be used in compliance with all applicable laws and regulations, including data protection, privacy, and intellectual property laws.

Refer to ISM.16: *AI Policy*.

14.3 Security policy

14.3.1 Security audits

Control: independent audits of security management and compliance will be carried out periodically or whenever major changes are made.

Such audits can be internal or by engaging an outside agency.

14.3.2 Security policy compliance

Control: managers must periodically review compliance with security policy within their areas of responsibility to ensure that policy and procedures are followed, and that all other security requirements are being met.

14.3.3 Technical compliance

Control: information processing facilities must be periodically reviewed for compliance with security policy and procedures.