Jardine Matheson

Information Security Policy

Jardine Matheson (Jardines) is an investment company dedicated to building a diverse portfolio of high-quality, scaled businesses in Asia Pacific. Jardines and our portfolio companies are committed to protecting information and supporting business operations by preserving the confidentiality, integrity, and availability of information assets. The Jardines information security programme is guided by internationally recognised standards and frameworks, including ISO/IEC 27001 and the NIST Cybersecurity Framework, adapted to Jardines' operating context and risk profile.

This Information Security Policy (the Policy) applies to employees, contractors, and third parties who access, process, store, or transmit information on behalf of Jardines, whether through on-premises or cloud services. This Policy sets out high-level principles for information security and should be read in conjunction with the internal standards and guidelines developed and disseminated by Jardines. Our portfolio companies, associated companies and joint venture partners are encouraged to adopt this Policy or incorporate its principles into their own policies where appropriate, proportionate to their risk profile and applicable legal or regulatory requirements.

We are committed to the following principles:

Governance and accountability

- The Board of each portfolio company is responsible for governing information security within its organisation and for ensuring that appropriate resources and oversight mechanisms are in place.
- Senior management is accountable for the implementation of the information security programme and for maintaining governance processes that coordinate security objectives across business and technology functions.
- Roles and responsibilities for information security are defined and reviewed periodically, encompassing governance, risk management, engineering, operations, compliance, and audit.
- The information security programme and its controls are subject to independent review by internal audit, external compliance auditors, or another function approved by the management of that business. Audit findings are tracked to resolution, and results are reported to the Board or an appropriate governance body.
- The effectiveness of information security governance is monitored on an ongoing basis to support continuous improvement.

Risk management

- Periodic risk assessments are performed to identify and manage risks to information and systems.
- Risk assessment outcomes inform control selection and prioritisation.

Security principles

- Security accountability – security is a shared responsibility at Jardines; individuals and teams are accountable for protecting information within their roles.
- Defense-in-depth – multiple layers of controls are used to reduce the likelihood and impact of threats.
- Least privilege – access is limited to what is necessary for authorised business purposes.
- Security by design – security requirements are considered throughout the lifecycle of systems and services
- Continuous improvement – controls are periodically tested, reviewed and improved as technology, threats, and business requirements evolve.

Framework alignment

- The information security programme is aligned with internationally recognised standards, including ISO/IEC 27001 and the NIST Cybersecurity Framework.
- These frameworks inform the selection, implementation, and assessment of security controls at Jardines.
- Framework alignment is adapted as needed to reflect specific business, regulatory, and risk contexts.

People and Culture

- Personnel security practices such as screening (as permitted by law), role-appropriate onboarding, and processes to address policy violations are maintained.
- Security awareness is provided to all personnel, including training on responsibilities, common threats such as social engineering, and how to report concerns.
- We strive to foster a culture in which every individual understands their role in protecting Jardines' information.

Information and asset management

- Information assets and supporting systems are assigned to owners and are managed through their lifecycle.
- Information is classified and handled according to its sensitivity (for example, public, internal use, confidential, and highly confidential).

- Information and media are disposed of securely when no longer required, using methods appropriate to sensitivity and legal obligations.

Access control

- Access to information and systems is governed by authorisation processes and reviewed periodically.
- Users are uniquely identifiable where feasible, and strong authentication controls, including multi-factor authentication for higher-risk access, are used where appropriate.
- Access is adjusted when roles change and is removed promptly when no longer needed, including on termination of employment or contract.

Cryptography and data protection

- Cryptographic protections appropriate to risk are used to help safeguard sensitive information at rest and in transit.
- Key management practices are maintained to support the effective use of cryptographic controls.

Physical and environmental security

- We maintain physical security controls to protect facilities and equipment against unauthorised access, damage, and disruption, commensurate with risk and business needs.

Operational security

- Systems are configured using security baselines where applicable, and changes affecting security are managed through controlled processes.
- Security-relevant events are logged and monitored to support detection, investigation, and response, with retention aligned with operational and regulatory needs.
- Processes to identify and address vulnerabilities and to employ protective controls against malicious software, using a risk-based approach
- Backups and recovery capabilities are maintained to support restoration of critical data and services and are tested periodically.

Network and communications security

- Network security controls are implemented to help protect communications across networks and to restrict access to systems and data through appropriate design, segmentation, and secure channels.

Secure development and technology change

- Security requirements are integrated into system acquisition, development, and maintenance, including practices such as threat assessment, testing of security functions prior to deployment, and management of third-party components.

Supplier and third-party security

- Third-party risks are managed by applying security expectations to suppliers and service providers, including due diligence, contractual security requirements, and ongoing oversight proportionate to risk.

Incident management

- Incident response capabilities are maintained to identify, assess, respond to, and recover from security incidents.
- Incident response includes defined processes, role assignments, and continuous improvement activities such as post-incident reviews; and
- Significant incidents are escalated and reported in accordance with applicable legal and regulatory requirements.

Business continuity and resilience

- Business continuity and resilience practices designed to sustain or restore critical services following disruptive events are maintained.
- Continuity plans are subject to governance oversight, and periodic exercising and testing aligned to business needs.

Compliance, privacy, and assurance

- We seek to comply with applicable legal, regulatory, and contractual requirements for information security and privacy.
- Monitoring and assessments are conducted to evaluate the effectiveness of the security programme.
- Effectiveness of security controls is validated through periodic offensive testing and independent assessments.

Policy exceptions

Exceptions to this Policy may be granted only when a documented business justification exists, the risk is assessed, compensating controls are defined where appropriate, and management approval and risk acceptance are recorded.

Contact

For enquiries about this Policy or to report a potential security concern, please contact the Jardine Matheson Cybersecurity team at infosecpolicy@jardines.com. This dedicated contact address is monitored by the Cybersecurity team and serves as the official channel for questions, feedback, or requests relating to this Policy.

This Policy has been endorsed by Executive Management and will be reviewed periodically and updated as required.