Information Security Policy

Security Management Australalasia

Contents

Section 1 – Introduction

Intent and Scope

This information security policy (**policy**) provides the basis of information security management within Security Management Australasia (**Company**). Effective protection of business information is vital for both preserving the reputation of the Company and reducing the risk of data falling into the wrong hands.

This policy aims to fulfil the following priorities:

1. Meet legislative requirements and execute due diligence in keeping internal and client data safe and secure.
2. Outline the Company standard for data storage, confidentiality, maintenance and disposal.
3. Ensure the integrity of the Company's data systems and assets.
4. Uphold the Company's reputation as a trusted recipient of data.
5. Maintain storage and back-up systems that meet the needs of the Company and its employees, contractors, volunteers, vendors and anyone else who may have any type of access to the Company's systems, software, hardware, data and/or documents (collectively referred to as the **Participants**).

Responsibilities

This policy applies to all Participants who are given access to the Company's systems, software, hardware, data and/or documents. All Participants are responsible for protecting business information and systems. Where there is any doubt about the security of any action, the Participants should contact the Security Team and take a cautious approach to avoid any potential risks. The Information Security Manager is responsible for implementing this policy, and can be contacted at security@smaust.com.au.

Section 2 – Data Security

General Security Requirements.

1. Participants must not install unauthorised software. The Company may at any time introduce a whitelist of approved/trusted programs. If this occurs, then only these programs may be used by the Participants.
2. Participants should stay up to date with any other Company-wide recommendations, such as recommended browser settings.
3. Participants should perform daily backups of important new/changed data, software, and configuration settings.

4. Participants must not attempt to turn off or circumvent any security measures, unless instructed to do so temporarily by the Operations or Information Security Managers for troubleshooting purposes.
5. Participants must report any security breaches, suspicious activities or issues that may cause a cyber security breach to the Security Team and await their instructions regarding the appropriate response to the breach.

Transferring Data

Data transfer is a common cause of cybercrime. The Participants should follow these best practices when transferring data:

1. Avoid transferring personal information such as customer data and employee information (this includes anything that can or may identify an individual including first name, last name, age, address, and email address) unnecessarily.
2. Adhere to relevant personal information legislation outlined in *The Privacy Act 1988*. Our privacy policy can be found at https://www.smaust.com.au/.
3. Data should only be shared over authorised networks and through authorised applications.

Working Remotely

When working remotely, the security requirements outlined in this policy must be followed. Phones and laptops used to access data must not be left unattended, and must be locked while not in use. Company files should only be accessed from Company provided devices unless otherwise approved by the Security Information Manager.

Clear Desk

All employees are required to clear their desks of any sensitive information at the end of each workday or whenever they are away from their desk for an extended period. This includes, but is not limited to, documents, notes, printouts, USB drives, and any other physical or electronic media containing sensitive information.

Company Systems

When accessing the internet from any Company systems:

1. Participants are not to intentionally circumvent any security measures.
2. Participants must take reasonable care when downloading documents, sending or receiving data (via emails or any other means), or accessing websites to ensure the sources are not malicious.

When accessing Company owned accounts (including Microsoft user accounts or accounts with vendors):

1. Accounts owned by the Company are only to be used for the Company purposes and not for personal use unless approved by management.

2. Participants are responsible for ensuring all sensitive information on their account is safeguarded according to Company guidelines; this includes their login and password information. Creating copies of sensitive information without the approval of management, or with the purpose of distributing it to unauthorised persons is prohibited.
3. Participants must not engage with Company accounts or systems with the intent of: bullying or harassment; degrading the system or Company relations with clients, vendors or third-parties; diverting Company resources for personal purposes; or accessing accounts, systems or information for which they do not have authorisation.

Retention and Disposal of Data

The Security Team are responsible for identifying assets, equipment, and information that are no longer needed or have reached the end of their useful life. In accordance with *The Privacy Act 1988, t*he Company will dispose of sensitive client and employee data as soon as it is no longer needed.

Participants should report any information they find that they believe to fit the criteria for disposal to the Security Team.

1. Prior to disposal, electronic devices, storage media, and IT equipment must undergo data sanitization procedures to ensure that all sensitive information is securely erased or destroyed. Data sanitization methods may include overwriting, physical destruction, or using certified data erasure software.
2. Assets and equipment that cannot be reused or repurposed must be physically destroyed to prevent unauthorized access or recovery of sensitive information. Destruction methods may include shredding, pulverizing, incineration, or disassembly, depending on the type of material and security requirements.
3. Disposal activities will be conducted in accordance with environmental regulations and best practices to minimize the impact on the environment and promote sustainability.
4. Where required by legislation, records of disposal activities, including asset inventories, disposal logs, certificates of destruction, and disposal receipts, will be maintained for auditing and compliance purposes. Disposal records will document the date, method, location, and responsible party for each disposal activity.

Section 3 - IT Security

Password and Authentication Requirements

In order to safeguard Company assets and client information, these best practices for setting up passwords on Company owned accounts and systems should be followed:

1. Passwords set up by an administrator must be uniquely and randomly generated, then immediately changed by the user.
2. Use at least 12 characters (must contain capital and lower-case letters, numbers, and symbols).

3. Do not write down passwords and leave them unprotected.
4. Do not exchange credentials without manager approval.
5. Change passwords when there is any possibility that an existing password may have been compromised.
6. Use multifactor authentication tools wherever possible.
7. Only share passwords for shared accounts via the password manager appointed by the Information Security Team, and with approval of management.

Use of a password management tool is encouraged, whether integrated into a mobile app or an internet browser.

Email Security

Emails can contain malicious content and malware that could jeopardize employee and client information and Company systems. Participants should employ the following strategies:

1. Do not open attachments or click any links where content is not well explained.
2. Check the email addresses and names of senders and keep watch for anything suspicious in the body of the email.
3. Block junk, spam, and scam emails and report phishing and scams to the Security Team.
4. Avoid emails that contain common scam subject lines such as prizes, products, deals and money transfers.
5. Where an email requests financial payment, confirmation of password, or prompts to login to a Company system, extreme care should be taken to ensure that it is genuine, such as calling the sender and obtaining manager approval.

If a Participant is not sure that an email, or any other type of data or communication is safe, the Participant should contact a Security Team member.

Physical Security

1. All servers, mainframes and other network asset locations must be secured with appropriate access through RFID access tags. It will be the responsibility of the Information Security Manager to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the Security Team immediately.
2. The security of all Company owned portable technology devices, including laptops and phones, will be the responsibility of the employee who has been issued with the device. Each employee is required to use secure passwords, and where possible multifactor authentication, on the device and ensure the asset is kept safe to protect the security of the asset issued to them.
3. In the event of loss or damage of a device, the Information Security Manager will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage of the device.

4. All Company owned portable devices stored on site are to be secured by CCTV and RFID access.

Access Control

a. Access to our facilities will be controlled through access control systems, such as keycards or biometric readers.
b. Employees, visitors, and contractors must display proper identification badges or passes while on-site and adhere to the designated access control procedures.
c. Access to restricted areas within our facilities will be granted only to authorized personnel based on their job roles and responsibilities.
d. Visitors and guests should be escorted at all times while in areas containing sensitive information. Employees must ensure that visitors do not have access to confidential documents or electronic devices unless explicitly authorized.

Backups

The Security Team will ensure that all data held by the Company is regularly backed up. Backup schedules will be established based on business requirements, with consideration given to factors such as data volatility, regulatory compliance, and operational needs.

Backup retention periods will be defined based on regulatory requirements, business continuity objectives, and data recovery needs. Archived backups may be retained for longer periods to support historical data analysis, legal compliance, or audit purposes.

Backup data will be stored at geographically separate and secure off-site locations to protect against localized disasters, such as fires, floods, or physical theft. Off-site storage facilities will be equipped with appropriate security measures to safeguard backup media from unauthorized access or environmental hazards.

Backup data will be encrypted during transmission and storage to protect it from unauthorized access or interception. Encryption keys will be managed securely to prevent unauthorized decryption of backup data.

Encryption

The organization will utilize industry-standard encryption algorithms and protocols to protect sensitive data, such as Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), RSA, and Elliptic Curve Cryptography (ECC). Encryption algorithms and key lengths will be selected based on security best practices, regulatory requirements, and the sensitivity of the data being protected.

All sensitive data stored on electronic devices, servers, databases, and removable media must be encrypted using approved encryption methods. Full disk encryption (FDE) or file-level encryption will be implemented to protect data at rest from unauthorized access in the event of theft, loss, or unauthorized access.

Sensitive data transmitted over networks, including internet connections, wireless networks, and virtual private networks (VPNs), must be encrypted using secure transport layer protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL). Encryption protocols will be configured to use strong encryption ciphers and key exchange mechanisms to prevent interception, eavesdropping, and man-in-the-middle attacks.

Email communications containing sensitive or confidential information must be encrypted using secure email encryption protocols, such as Pretty Good Privacy (PGP), Secure Multipurpose Internet Mail Extensions (S/MIME), or Transport Layer Security (TLS). Employees will be provided with encrypted email solutions or instructed on how to use encryption features in their email clients to protect sensitive communications.

- Encryption keys will be generated using cryptographically secure random number generators to ensure randomness and unpredictability. Key generation processes will adhere to established cryptographic standards and guidelines to maintain the strength and integrity of encryption keys.
- Encryption keys will be securely stored and protected from unauthorized access, loss, theft, or tampering. Key management systems and hardware security modules (HSMs) may be used to safeguard encryption keys and manage access controls.
- Encryption keys will be rotated periodically to minimize the risk of key compromise and ensure the long-term security of encrypted data. Key rotation schedules will be established based on industry best practices, regulatory requirements, and risk assessments.
- Encryption must be used for all sensitive data, communications, and systems as defined by organizational policies, regulatory requirements, and data classification standards. Employees are responsible for identifying and encrypting sensitive information in accordance with organizational guidelines and encryption policies.
- Access to encrypted data, systems, and encryption keys will be restricted to authorized personnel based on the principle of least privilege. Encryption keys will be accessible only to individuals with a legitimate business need and proper authorization to decrypt encrypted data.
- Regular compliance audits and assessments will be conducted to verify adherence to encryption policies, standards, and controls. Audits may include reviewing encryption configurations, key management practices, encryption usage, and compliance with regulatory requirements.
- Security monitoring systems will be deployed to detect and report any unauthorized attempts to access, modify, or bypass encryption controls. Anomalies, security incidents, and encryption-related events will be logged, analyzed, and investigated to identify potential security risks or vulnerabilities.

Section 4 - HR Security

Authorisation and Access

Managers should grant authority and access to Participants on a need-to-know basis where possible. Caution should be taken when:

- Sharing information and documents with the Participants.
- Authorising the Participants to enter and control information systems.
- Giving the Participants access to sensitive data.

If there is any uncertainty regarding what qualifies as need-to-know, contact the Information Security Officer.

Exiting

Access to all systems – both physical and digital – should be revoked within twenty-four hours of a Participant leaving the employ of the Company. Devices solely used by the Participant should be vetted for any data, then digitally sanitized and repurposed.

Data Confidentiality and Integrity

All HR data will be treated as confidential and disclosed only to authorized individuals on a need-to-know basis. Employees are prohibited from sharing HR information with unauthorized parties, including colleagues who do not have a legitimate business need for the information. Confidential HR data will be encrypted when transmitted electronically and stored securely to prevent unauthorized access.

HR data will be accurate, complete, and up to date to ensure its integrity and reliability for decision-making purposes. Any changes or updates to HR data will be recorded, and appropriate controls will be in place to prevent unauthorized alterations. Regular audits and reviews will be conducted to verify the accuracy and completeness of HR records.

Retention and disposal guidelines are outlined on page 5.

Employee Privacy

The organization respects the privacy rights of its employees and complies with applicable privacy laws and regulations. Employees have the right to access their own HR data and request corrections or updates, as necessary. HR data will not be used for purposes other than those outlined in this policy or as required by law.

Incident Reporting

Employees are required to report any suspected or actual security incidents involving HR data to the Information Security Manager immediately.

An incident response plan will be in place to promptly investigate and mitigate security breaches involving HR data, including appropriate notification of affected individuals and regulatory authorities as required.

Section 5 – Maintenance, Training and Review

Other Company Policies

This Policy must be followed in conjunction with the Company's other policies, which can be accessed at https://www.smaust.com.au/.

Training

All Participants must maintain working knowledge of basic information security protocols. All new Participants will be given training on information security.

Disciplinary Action

If this policy is breached, one or more of the following disciplinary actions will take place:

a. In case of breaches that are intentional or repeated or cases that cause direct harm to the Company, Participants may face serious disciplinary action, including the termination of employment, engagement, or services.
b. Subject to the gravity of the breach, formal warnings may be issued to the offending Participants.

Incidents will be assessed on a case-by-case basis.

Review

The Company will periodically review this policy and update as required to ensure the continued security of the Company. It is important for the Participants to stay up to date with changes to this policy.

Controlled Document Reference: **012405SMAISP**	Issue: 1	Revision: 0
Review Period: Annual	Next Review Date: 2025	
Document Controller: **Faye Pirie - Compliance Manager**		
Document Owner: **Stephen Sjepcevich - Operations Manager**		Approved: **2024**