SAAFE Limited Information Security Policy

1. Scope

This Policy applies to all SAAFE Ltd. personnel and anyone who has access to SAAFE Ltd.'s data and technology infrastructure. It encompasses all aspects of the Research Program, emphasising the importance of risk assessment and the implementation of appropriate controls. Partner organizations are required to conduct their own information security risk assessments and establish systems for managing cyber risks to maintain compliance.

2. Introduction

In today's digital landscape, safeguarding information assets is vital. SAAFE Ltd. has established a robust Information Security Policy to ensure the confidentiality, integrity, and availability of its data and technology. The Board of Directors maintains a conservative appetite for risk in this area, committed to minimizing exposure to threats and vulnerabilities. This policy is a key component of SAAFE Ltd.'s governance framework and demonstrates a commitment to protecting sensitive information. The Board, along with the Audit, Risk, and Finance Committee, is responsible for reviewing this document, coordinating with the Executive and Management Level for ongoing document maintenance and alignment with the organisation's risk profile.

3. Purpose and Objective

The purpose of this policy is to safeguard the confidentiality, integrity, and availability of all electronic information that SAAFE Ltd. creates, receives, maintains, or transmits. By upholding stringent security principles and aligning with regulatory standards, we are committed to ensuring that our data assets are protected against unauthorised access, disclosure, alteration, or destruction.

The objective of this policy is to formalise a comprehensive Information Security Policy in line with the recommendations and guidelines of the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC). It aligns with industry best practices and the ACSC's 'Essential 8 Maturity Model,' which covers key security domains.

This policy aims to achieve the following:

- Define the roles and responsibilities of SAAFE Ltd. personnel in safeguarding information assets.
- Promote a culture of information security awareness and responsibility throughout the organisation.
- Establish guidelines for the secure handling, storage, and sharing of sensitive information.
- Ensure compliance with relevant legislative and regulatory requirements.

- Ensure appropriate measures are put in place to mitigate security risks associated with data breaches, unauthorised access, and system vulnerabilities.
- Minimise the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by third parties.

4. Definitions

Term	**Definition**
Information Security	The practice of protecting information from unauthorised access, use, disclosure, disruption, modification, or destruction to ensure its confidentiality, integrity, and availability.
Data Breach	An incident where unauthorised individuals gain access to sensitive or confidential data, potentially resulting in its exposure, loss, or misuse.
Risk Assessment	The process of identifying and evaluating potential risks and vulnerabilities to determine the likelihood and impact of security incidents.
Sensitive Information	Data that, if compromised or disclosed, could lead to harm, financial loss, legal or regulatory penalties, reputational damage, or a violation of privacy.
Information Security Policy	A set of guidelines, rules, and procedures that govern the protection of information assets within an organisation.
Data Storage Services	Technology platforms or systems used for the storage, management, and access of data, ensuring its security and availability.
Information asset	An information asset is information (physical or digital) and information systems, including software and hardware, through which information is stored, accessed modified or transferred. Information assets include both structured information (such as a database) and unstructured information (such as emails). Information assets may include • Records, regardless of formation (eg emails, documents, spreadsheets, images etc) • Databases and other information technology systems or infrastructure in which data is stored, accessed or transferred. • Devices, such as laptops, through which data can be accessed, input, amended, deleted, extracted or analysed. • Ancillary systems such as environmental control systems or physical access control systems.

Term	Definition
ASD Essential Eight	The ASD Essential Eight is a cybersecurity strategy devised by the Australian Signals Directorate (ASD). It consists of a set of eight fundamental mitigation strategies that organisations can implement to improve their cybersecurity posture. SAAFE Ltd.'s IT provider and cyber security specialists have developed the SAAFE Ltd. IT Environment to comply with level 1 of these controls (we exceed level 1 in some areas)
CIS 18 Security Controls	The Center for Internet Security (CIS) Controls are a set of best practices designed to help organisations bolster their cybersecurity. Originally consisting of 20 controls, they were later revised and condensed into 18 security controls. These controls provide SAAFE Ltd. CRC more guidance with regards to managing cybersecurity. SAAFE Ltd. has conducted a review to highlight alignment and potential gaps in control.

5. Responsibilities

Everyone in the organisation plays an important role in the protection of SAAFE Ltd.'s Information Security to ensure that SAAFE Ltd. continues to provide the level of data security and assurance typical of a best in class Australian Cooperative Research Centre.

The table below outlines the various roles and responsibilities SAAFE Ltd. have in place to assist in managing these controls:

Level	Role	Responsibilities
Board Level	Board of Directors	• Establishing cybersecurity governance and policies • Overseeing risk management and compliance • Allocating resources for cybersecurity measures • Ensuring alignment with legal and regulatory requirements
	Audit, Finance, and Risk Committee	• Reviewing and evaluating cybersecurity risks • Ensuring alignment with financial regulations and controls • Coordinating with executive and management level for audit and risk assessments
Executive & Management Level	Chief Information Security Officer (CISO) / IT Security Manager	• Developing and implementing a cybersecurity strategy, policies and procedures • Managing security technologies, vendors, and teams • Overseeing security training and awareness programs • Coordinating incident response and remediation • Conducting security assessments and audits • Monitoring security alerts and threats • Collaborating with IT teams on security enhancements • Reporting to the board on security status and incidents

Level	Role	Responsibilities
Operational Level	Cybersecurity Analyst / Department Heads	- Implementing cybersecurity policies and procedures - Monitoring security alerts and threats - Conducting security assessments and audits - Collaborating with IT teams on security enhancements - Ensuring departmental compliance with security policies - Encouraging security awareness within the department
External Partners	Comunet (IT Providers and Information Security Specialists)	- Providing IT solutions and security technologies - Offering specialised cybersecurity consulting and services - Collaborating with internal teams for security alignment and enhancement - Supporting incident response and remediation efforts
Employee Level	All Staff	- Adhering to organisational cybersecurity policies and procedures - Reporting suspicious activities or incidents - Participating in security awareness training - Practicing safe online behaviors and securing sensitive information

6. Scope and Role of Risk Assessment

The Risk Assessment Tool and set of Information Security Expectations provided with the Project Partner Pack will enable Partner Organisations to understand their Information Security risk profile, encouraging them to identify high risks related to:

- Data asset sensitivity – Example considerations - Is this personal data, research program data, or the football scores?
- Data storage protections – Example considerations - Is this location behind an Australian University firewall, or is it an old server that nobody is sure who has access, or is it a personal laptop
- People related information risk – Example considerations – Is this data protected by password / MFA? Do only the people that need to see this data have access?

If, after conducting their initial Data Security Risk Assessment, Project Partners are returning unmitigated risks, SAAFE Ltd. CRC will liaise with the partner on the issue in question until appropriate control measures are in place.

7. Policy Compliance

7.1. Essential 8 Compliance

SAAFE Ltd.'s Network Administrators, Comunet, will maintain systems to ensure compliance with the Australian Cyber Security Centre's (ACSC) Essential Eight. Currently, SAAFE Ltd. have controls consistent with Maturity Level One. Maturity level positioning and compliance will be discussed on an 'as needs' basis or annually at the Q4 Data Breach Response Team meeting (which includes Comunet Cyber Expert).

Compliance with the Essential 8 maturity framework includes installing, implementing, and maintaining firewalls, anti-malware software, application controls, systems for application hardening, automation of application and operating system patching, control of macro settings and regular backups.

Compliance with the ACSC Essential 8 requirements also meets the network security requirements of the Defence Industry Security Program.

7.2. The 18 CIS Critical Security Controls

The Center for Internet Security (CIS) Controls are a set of best practices designed to help organizations bolster their cybersecurity. Originally consisting of 20 controls, they were later revised and condensed into 18 security controls. These controls provide SAAFE Ltd. more guidance with regards to managing cybersecurity. SAAFE Ltd. has conducted a review to of compliance with the 18 CIS Critical Security Controls and either is currently compliant or is working towards compliance across all areas, with the exception of CIS 18 – the conducting of third-party penetration tests. A third-party system audit will be conducted to determine if compliance with this is required. An overview of the requirements of the CIS Security Controls and out compliance with them is available in the separate document MWF-4-7-CIS 18 Compliance Position v0.1.

8. Policy Elements

8.1. User Access Management

- Onboarding: Employees are provided access to systems and data based on job roles and responsibilities. Access controls and policy implementation are documented and reviewed within 3 months of the employee commencing, and regularly thereafter.
- Offboarding: When employees leave the company, all access rights are promptly revoked, and any company-owned assets are returned.

8.2. Unacceptable Use, Limited Personal Use, Email Guidelines and monitoring:

- Limited Personal Use: Employees are allowed infrequent and brief personal use that doesn’t interfere with work responsibilities, operation of the company, security, storage capacity, network performance, and that complies with Social Media Policy and other IT Policies and Procedures.
- Use of Private Email: SAAFE Ltd. staff must strictly adhere to using the designated company email accounts for all official correspondence, including but not limited to sensitive information, data, passwords, or confidential documents. Personal email accounts must not be used for any business-related purposes and should neither be stored on, sent from, nor sent to SAAFE Ltd. computers or devices.
- Unacceptable Use: Includes activities like unlawful or offensive communication, visiting inappropriate websites, unauthorized exchange of company information, copyright violation, online gambling, advertising, defamation, misrepresentation of the company, anonymous or unauthorized email transmission, personal commercial interests, gaming, etc.
- SAAFE Ltd. establishes the company’s right to review and monitor electronic records, including using computer surveillance if needed, all in accordance with appropriate legislation. This monitoring may include, but is not limited to, internet browsing history, email content and metadata, file access and transfers, and system and network activity logs. The purpose of this surveillance is to ensure compliance with company policies, protect company assets, and support the investigation of improper access and use.

8.3. Password Management and Review

- Passwords are required to meet complexity and length standards.
- Regular reviews and changes are mandated for Admin passwords.
- Processes are in place for revoking access to systems from contractors or departed staff.

8.4. Patch Management

- Regular assessments are conducted to identify required security patches.
- Patches are systematically tested and deployed in accordance with the organization's risk profile and compliance requirements.

8.5. Physical Security of Information Assets

- Asset control procedures govern the management of physical assets (laptop return etc).
- Secure disposal methods are enforced (Comunet Laptop Wipe etc).
- Building access controls are maintained.

8.6. Unauthorised Software and Equipment

- SAAFE Ltd. strictly prohibits the downloading, installation, or use of unauthorized software, programs, or hardware within the company's network and devices.

8.7. Management of Mobile and Portable Devices

- Devices must adhere to organizational security policies and guidelines.
- Loss or theft of devices must be promptly reported.
- Mobile device management (MDM) solutions are utilized to ensure compliance and remote management.

8.8. Foreign Networks

SAAFE Ltd. staff will not connect SAAFE Ltd. devices to foreign networks. If working away from the office, SAAFE Ltd. staff will access the internet using 'Personal Hotspot' on their mobile phone, with password protection.

8.9. Risk Assessment for Data Storage

SAAFE Ltd. staff and research project participants must store sensitive research data in approved storage services that have been checked for security risks (e.g., Office 365 Microsoft Teams Environment). A template for mapping this data is included in the Project Reporting Pack. Only information considered highly sensitive needs to be mapped this way. This mapping is required for specific projects, and SAAFE Ltd. may review or audit the data map as needed.

8.10. Copyright and Intellectual Property Rights Compliance

SAAFE Ltd. enforces respect for copyright and intellectual property rights, in compliance with the Copyright Act 1968 and other relevant intellectual property laws. Employees must ensure that they use intellectual property, including software, documents, music, images, and other copyrighted material, in a manner that does not infringe upon the rights of the owners. Unauthorized copying, distribution, modification, or use of copyrighted material is strictly prohibited. This includes obtaining proper licensing for software and other proprietary content. All actions must align with the legal requirements concerning intellectual property rights and must adhere to the company's commitment to lawful and ethical conduct.

8.11. Use of Email for Sensitive Information

SAAFE Ltd. staff will not transfer sensitive information such as data or passwords via email. Rather, information will be shared via email links to files stored in the SAAFE Ltd. Office 365 Teams Environment or by providing links to this location in SAAFE Ltd.'s task management system, ClickUp.

8.12. Two Factor Authentication (2FA)

It is an expectation that SAAFE Ltd. staff use 2FA on all supporting software and services. It is an expectation that SAAFE Ltd. use Bitwarden password protection software, or similar, to store passwords and login information related to software and services associated with SAAFE Ltd..

9. Training

Induction: At induction, SAAFE Ltd. will provide training on the content of this policy and provide the policy itself within the Employee Policy Handbook.

As a regular annual event, SAAFE Ltd. will maintain and provide Information Security training and expectations to all Head Office Staff. The SAAFE Ltd. Operations team is responsible for this.

Upon Project Contracting, SAAFE Ltd. will make this training available for Partner Organisations. The SAAFE Ltd. Operations function is responsible for running this training with SAAFE Ltd. head office staff and for making it available to partner organisations (via Slide deck in Partner Project Pack).

Comunet will also inform Personnel regularly about new scam emails or viruses and ways to combat them.

10. **Reporting and Management of Potential Data Breaches**

Personnel should report potential, perceived or actual cyber-attacks, suspicious emails or phishing attempts, or other potential loss of data (such as misplaced laptops) as soon as possible to the Network Administrator who will investigate and resolve the issue promptly and send a company-wide alert when necessary.

SAAFE Ltd. has a Data Breach Response Plan that outlines the process for managing any potential data breach or will provision the establishment of a Data Breach Response Team tasked with ensuring the SAAFE Ltd. Data Breach Response plan is a well-understood and effective mechanism for ensuring an appropriate response in the event of a data breach.

A representative from the Comunet team will be included in Data Breach Response Team Proceedings and will help investigate security breaches thoroughly.

11. Continuous Improvement

To continually adapt and improve this policy a number of actions will be taken over the next twelve months (through to June 2024) including:

- Annual review of the policy in conjunction with any recommended actions from the completion of the ACSC Cyber Security Risk Tool
- Consultation with relevant stakeholders (e.g., federal and state Health Departments, Department of Agriculture and Fishing and Forestry) about the content of this policy and any additional measures required
- An audit of this policy and the data security measures outlined in it will be audited for completeness by an appropriate third-party expert consultant.

- SAAFE Ltd. investigate the test options in Microsoft Defender for protection and training against Phishing.

12. Related Documents

This Information Security Policy should be read in conjunction with the following documentation:

- SAAFE Ltd. Data Breach Response Plan - Defines the steps and procedures to be followed in the event of a data breach.
- SAAFE Ltd. Ltd Privacy Policy - Outlines the principles and guidelines for the collection, use, and protection of personal information within SAAFE Ltd..
- SAAFE Ltd. CRC Project Risk Register and Data Storage Map.xls outlines the specific sensitive data being collected by projects and the requirements of their storage locations.