CYBER SECURITY AND INFORMATION SYSTEMS POLICY

On Behalf of the ED and Board by: Chief Operating Officer

Approved by the Board: 22 December 2023

Contents

Cyber and Information Security Policy and Procedures

1. Introduction

1.1 While AAA wishes to foster a culture of openness, trust, and integrity, this can only be achieved if external threats to the integrity of the organisation's systems are controlled and the organisation is protected against the damaging actions of others

2. Purpose

2.1 This policy sets out guidelines for generating, implementing and maintaining practices that protect the organisation's cyber and information media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

2.2 This policy applies to employees, contractors, consultants, and volunteers at AAA, including all personnel affiliated with third parties, to all equipment owned or leased by AAA, and to all equipment authorised by AAA for the conduct of the organisation's business

3. Policy

3.1 While AAA wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the organisation's systems remains the property of AAA. Because of the need to protect AAA's network, the confidentiality of information stored on any network device belonging to AAA cannot be guaranteed, and AAA reserves the right to audit networks and systems periodically to ensure compliance with this policy.

3.2 Employees and volunteers will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

3.3 Breach of this policy by any employee may result in disciplinary action, up to and including dismissal.

Cyber Security Procedures

1. Responsibilities

1.1 It is the responsibility of the CEO to ensure that:

- staff are aware of this policy;
- any breaches of this policy coming to the attention of management are dealt with appropriately;
- the COO to take up the role of Cyber Security Officer.

1.2 It is the responsibility of the COO to ensure that:

- the CEO is kept aware of any changes to the organisation's cyber security requirements;
- a report on the organisation's cyber security is submitted annually to the board.

1.3 It is the responsibility of all employees and volunteers to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

1.4 In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures in any particular instance, employees and volunteers should consult their supervisor.

2. Processes

Monitoring

2.1 The CEO may authorise individuals with responsibility for cyber security issues in the organisation, including the COO, to monitor the organisation's equipment, systems and network traffic at any time for security and network maintenance purposes.

Confidentiality

2.2 Following consultation with the COO, the CEO shall from time to time issue cyber security procedures appropriate to different levels of confidentiality.

2.3 The organisation shall classify the information it controls in the organisation's computer system files and databases as either non-confidential (open to public access) or confidential (in one or many catogories).

2.4 The COO along with the Privacy Officer are required to review and approve the classification of the information and determine the appropriate level of security that will best protect it.

Access control

2.5 Individuals shall be assigned clearance to particular levels of access to the organisation's information resources, and shall access only those recourses that they have clearance for. Access control shall be exercised through username and password controls.

Computer security

2.6 All PCs, laptops and workstations should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

2.7 Users must keep passwords secure. Accounts must not be shared, and no other people may be permitted to use the account. Passwords should not be readily accessible in the area of the computer concerned. Authorised users are responsible for the security of their passwords and accounts.

2.8 Users who forget their password must call the Managed Service provider to get a new password assigned to their account.

2.9 Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorised users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

2.10 Users will not be allowed to log-on as system administrators. Users who need this level of access to production systems must request a special access account as outlined elsewhere in this document.

2.11 Employee log-on IDs and passwords will be deactivated as soon as part of the employee exit process.

2.12 Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the organisation's cyber security officer. Monitoring of the special access accounts shall be undertaken via the periodic generating of reports to the cyber security officer showing who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 30 days and will not be automatically renewed without written permission.

2.13 All computers and devices used by the user that are connected to the AAA internet/intranet/extranet, whether owned by the user or AAA, will be monitored continuously by virus-scanning software with a current virus database approved by the AAI/COO.

2.14 Malware protection software must not be disabled or bypassed, nor the settings adjusted to reduce their effectiveness.

2.15 Automatic daily updating of the malware protection software and its data files must be enabled.

2.16 All email attachments must be scanned. All documents imported into the computer system must be scanned. Weekly scanning of all computers should be enabled

2.17 Users should allow regular patch and antivirus updates as prompted by the system

2.18 Physical documents containing sensitive information must be securely disposed.

2.19 Where possible, sensitive data should not be removed from the organisation's premises without specific authorisation.

2.20 Staff must regularly manage documents in shared locations and delete files and folders that are no longer required

2.21 Alternatively, staff who need access to sensitive data offsite should be given remote access privileges subject to adequate safeguards.

2.22 Computers being deaccessioned (whether for sale, reuse or disposal) shall not be released until all data has been securely deleted.

2.23 Users shall not download unauthorised software from the internet onto their PCs or workstations.

2.24 Users must use extreme caution when opening email attachments received from unknown senders; these may contain viruses, malware or Trojan horse code.

2.25 Users who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the COO immediately. The user shall not turn off the computer or delete suspicious files.

2.26 Users shall not attach unauthorised devices to their computers unless they have received specific authorisation from their Manager or COO.

2.27 users must not:

a. Follow web-links or instructions provided by email, unless certain of their origin and function;
b. Send AAA's information through unauthorised messaging applications or social media platforms (e.g. WhatsApp, Facebook, etc.)
c. Send messages or download content that support illegal or unethical activities;
d. Change the security settings of their email software or Internet browser on a AAA device (e.g. laptop, desktop);
e. Send sensitive such as "Confidential", "Restricted" information via unencrypted email;

f. Send emails containing passwords in clear text, or account information such as log-on ID and password combinations;

g. Use corporate devices or identities to browse, search or interact with the dark web, such as those that require the Tor web browser.

Social Media Use

2.28 Staff/volunteers are trusted to act responsibly when using social media sites such as Facebook, Twitter, wikis, blogs, YouTube, and LinkedIn.

2.29 AAA information must only be shared over official, authorised communication channels.

2.30 When accessing social media sites on AAA computers or devices:

a. Staff may be subject to logging and monitoring checks;

b. Access may be restricted to social media sites; and

c. Inappropriate social media websites will be blocked.

2.33 When accessing or contributing on social media sites, staff must:

a. Not place comments representing or giving the impression of representing AAA, unless explicitly authorised to do so.

b. Exercise good judgement when blogging or posting.

c. Not post or view material that is illegal, obscene, defamatory, threatening, harassing, discriminatory, racist, or hateful to another person or entity.

d. Be aware that information hosted on social media is unverified and must not be used without confirming its authenticity for decision making.

2.34 AAA information must not be sent via unauthorised messaging platforms based on its classification and sensitivity (e.g. WhatsApp, Facebook Messenger, WeChat, etc.) and must only be transmitted using AAA approved and authorised messaging systems.

BYOD Devices

2.35 "Privately Owned or Bring Your Own Devices (BYOD)" devices are to be used where controls have been implemented to manage AAA's information on such devices e.g., information storage policies.

2.36 The user to ensure that the device is secured by a reasonable anti-virus software.

2.37 Official information is not to be downloaded on the device.

2.38 Upon termination of employment, all AAA information and access is removed from the device, and AAA may request inspection prior to departure.

Remote Access

2.39 When working from home or at an offsite location, staff:

a. Must never provide their login or email password to anyone, not even family members;

b. Must keep conversations confidential. Don't discuss work issues where others may hear, including elevators and lobbies;

c. Must not use personal email or cloud storage accounts for work;

d. Must make sure their home WiFi is password protected;

e. Must always lock laptop screen before stepping away — and use a laptop lock if in an unsecured area.

System and Network Security

2.40 AAA staff must not:

a. attempt to compromise the security of a computer;

b. access data, a server, or an account for any purpose other than for AAA duties or business, even if access is authorised, unnecessary access is prohibited;

c. export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management should be consulted prior to export of any material that is in question;

d. introduce malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.);

e. reveal account passwords to others or allow use of individual accounts by others. This includes family and other household members when work is being done at home;

f. use a AAA system / asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction;

g. make fraudulent offers of products, items, or services originating from any AAA account;

h. breach security controls or disrupt network communication (except for IT or security staff responsible for maintenance and troubleshooting). For the purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

i. port scanning or security scanning is expressly prohibited with the exemption of the IT team;

j. execute any form of network monitoring that will intercept data not intended for the end user's host, unless this activity is a part of the end user's normal job/duty;

k. circumvent user authentication or security of any host, network, or account;

l. interfere with or deny service to any user other than the AAA's host (for example, denial of service attack);

m. use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the internet/intranet/extranet'

n. provide information about, or lists of, AAA staff to parties outside AAA unless already classified as "public", and;

o. Attempt to attach any unauthorised device to the AAA business network.

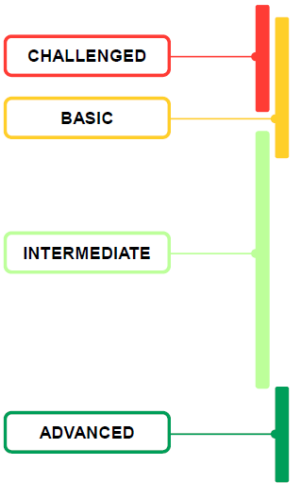
Appendix 1

Cyber security maturity model

Category	Challenged	Basic	Intermediate	Advanced
User access & authentication	User accounts are not well managed.	MFA is effectively configured on Microsoft 365/Google Workspace & sensitive internet-facing systems. Shared user accounts are eliminated or minimised & effectively managed (e.g. pswd vault). System access is reviewed on a scheduled basis.	Strong passwords are required. Processes exist to manage account breach risk – e.g. alerts, lockouts and/or log review. Admin rights are minimised, requires approval, time limited & protected (via MFA, VPN, SSH, etc.)	Access to important IT systems/applications employs Single-Sign on a secure, core authentication service.
Information classification & security	Information is not classified and the backup approach for information stores has not been thought through.	Data backup has been considered and configured as appropriate for all important information stores. A simple data recovery test is performed annually.	Information categories are defined (sensitive, confidential, public, etc.) and effectively used by staff (e.g., sensitive data is stored in an encrypted system). A system register records approved information categories for each system. Backups are reliable, secure and meet retention / recovery requirements. A significant restore is performed annually.	Technical controls restrict staff from storing or transmitting sensitive data incorrectly. Data retention requirements are known and addressed in line with organisational needs and compliance obligations.
Device & network management	Device security and network threats are not managed.	Windows PCs have antivirus protection. Only vendor-supported operating systems & applications are used. Device OS & applications are reliably patched through manual or auto-update processes. Default infrastructure admin passwords have been changed.	User devices have appropriate, centrally monitored firewall & antivirus software. Sensitive information is securely encrypted & can be remote-wiped. Patch management is undertaken centrally. Critical patches are deployed rapidly. Perimeter firewall and Wi-Fi configuration minimises security risk.	A process to identify, prioritise & manage technical vulnerabilities exists. A vulnerability scanner is used effectively. Devices that don't comply with policies (encryption, patching etc) are blocked. Devices are built & maintained to best practices standards (least privilege access, secure baselines, logging, etc.)
Polices, risk management & compliance	Policies and compliance processes are not well established.	End-user security, information security and privacy policies exist. Third parties with access to the organisation's information are required to keep information safe. Cyber security risks and protections are discussed at the executive level at least twice annually.	An assessment against the ACSC's Essential Eight has been performed and key risk addressed. An effective security risk management process exists. Annual security tests identify & remediate risks. A security incident response process is defined. Appropriate steps are taken to meet all legal, regulatory & contractual obligations.	The organisation has been independently assessed and confirmed as compliant against an information security standard such as ISO/IEC 27001.
User Education	Staff educate themselves.	Induction & annual refresh training effectively covers staff obligations, security risks BYOD, good password practice, sensitive information & who to contact for help.	Quizzes or phishing tests check knowledge annually. Specific training & processes support high-risk staff (accounts, CEO, CFO, IT, etc.) – e.g. phone call required to verify bank account changes.	Training is engaging, tailored by role, available on demand & effective. A strong security culture exists – staff actively consider it their responsibility.

Cyber security roadmap

Cyber security is a process of ongoing improvement, starting from where you are now. Once you assess your current stance, and your goal, start progressively working though successive stages.



1. Get the basic protections in place – multi-factor authentication, patching, user education, data backups, spam filtering, antivirus, firewalls and user accounts are confirmed
2. Begin the governance journey - develop and communicate an end-user security policy while engaging also the management team to manage cyber security risks
3. Classify organisation's information, define where it should be stored, how it must be protected and control who has access to it
4. Enhance the organisation's cyber security protections – improve patch and asset management, password practices, user access rights, administrative privileges and incident response processes
5. The organisation's legal, regulatory & contractual obligations are understood, and reasonable steps are taken to comply
6. Strengthen your backup protections and document these
7. Assess the organisation against the Australian Cyber Security Centre's Essential Eight and mitigate important risks
8. Implement a risk-based approach to managing cyber security, validated by planned penetration tests, phishing tests, vulnerability scans
9. Continue the cyber security journey through a continuous improvement program, and certification to external security standards.