ADMINISTRATIVE BRANCH POLICY STATEMENT 3.14

I.T AND DATA SECURITY FRAMEWORK

1. INTRODUCTION

1.1 Cyber security is critical to ensure the confidentiality, security and privacy of information by protecting against malicious threats and accidental incidents. Cyber attacks can exploit weaknesses in technology, people and processes to access information. Poor adherence to policies and procedures can result in ADAVB manages cyber security risk and conforms to relevant policies and regulations to protect the integrity of its data.

1.2 This policy establishes ADAVB's IT and Data Security Framework and is based on the principle that cyber security is a critical part of the association's function. Management of cyber security risk requires an ongoing effort across the organisation, and staff are required to be vigilant against security threats and handle technology assets and data with diligence. Also see Appendix 1: Incident Repsonse Plan.

1.3 Cyber security controls are designed to minimise risk by reducing the likelihood or impact of an incident or both. ADAVB will continue to identify and mitigate cyber security risks via the following measures:

- A register of key information assets.
- Maintaining a register of cyber security risks with related controls.
- Reviewing risks at regular intervals and as a result of significant security incidents, threats or changes to business requirements.
- Implementing and strengthening controls to reduce risk.
- Conducting security reviews, inclusive of intrusion testing, on a regular schedule
- Evaluating the effectiveness of controls

2. LEGISLATION AND STANDARDS

2.1 Relevant legislation and Standards include:

- Health Records Act 2001 (Vic)
- Healthcare Identifiers Act 2010 (Cth)
- My Health Records Act 2012 (Cth)

Reg'd Association No: A0022649E
ARBN: 152 948680

- Privacy Act 1988 (Cth)
- Spam Act 2003 (Cth)
- ISO/IEC 27033

3. SCOPE

This policy or relevant parts of this policy applies to anyone who has access to ADAVB data or information, including:

- ADAVB staff.
- ADAVB councillors and committee members.
- Third parties include but are not limited to IT consultants, vendors, managed service providers and partner organisations.

4. DATA

Confidential data is defined as any information that is not intended for public dissemination. This can be understood from three aspects:

- ADAVB protects its data, such as internal communications, policy and procedures and financial data.
- ADAVB protects the data of others, including personally identifiable data, such as those belonging to staff and stakeholders (this data is also protected under applicable laws and regulations for handling such information).
- ADAVB has a positive duty to protect member data, such as personally identifiable information and communications.

4.1 Specific Data Definitions

Depending on the aspect, **data confidentiality** is divided into three categories that result in different requirements for protecting the data, inclusive of:

4.1.1 Personally identifiable data and sensitive personal data

- Data that can identify a member, staff or stakeholder, such as name, residential address, insurance details and identity document information.
- IT user data, such as the access ID and password.
- IT utilisation data (log data related to the utilisation of ADAVB IT services).

4.1.2 Intellectual property

- Research information, communications and material that is not public.

4.1.3 Business-critical data

- Business-critical data includes any internal information accessible by specific groups of people. This includes strategic documents, accounting/financial data, information about members, benefactors, and foundations, legal matters and negotiations, and defence information.
- Business-critical data will be available to only a few select staff and protected from access by unauthorised personnel.

Reg'd Association No: A0022649E
ARBN: 152 948680

4.1.4 Other internal data

- Any non-public data that does not fall under one of the above categories should be referred to from this point on as other internal ADAVB data.
- This data is protected against external access but may be viewed by staff and stakeholders.

5. IT AND DATA SECURITY MANAGEMENT PROCEDURES

5.1 Vulnerability Testing

Security and/or intrusion testing will be performed against systems, processes, and people to determine their vulnerability to cyber threats. These test processes will be used to measure and improve service quality and protection against cyber threats. Testing is completed once a year, but more often is required. If circumstances require, automated testing that can be done each quarter will be introduced.

5.2 Unauthorised Access Monitoring

Monitoring unauthorised access, defined as an attempt by a party or parties not authorised to access the ADAVB domains, networks, or applications, is conducted monthly. The results are reported to management and, if required, the Council and Finance, Risk, and Audit Committee.

5.3 Dark web monitoring

ADAVB will monitor the appearance of access credentials of staff, ex-staff, Council and Committee members, and third parties on the dark web. If such credentials are listed, the person affected will require a password change. This may be a forced change at the direction of the Business Operations Manager

5.4 Access and Log in Requirements

ADAVB has access standards, user identification and passwords, that meet strict cyber security standards.

- Staff and other stakeholders onboarded to the ADAVB's systems will be provided user identification and log in credentials.
- All user identification and passwords are revoked when the staff leaves the organisation or the stakeholder no longer requires access to the associations network and , applications.

5.5 Passwords

- Must conform to the minimum length and complexity standard set by the ADAVB and updated when.
- All passwords will generally be required to have upper and lower-case letters, symbols and numbers.
- Multifactor authentication will be enabled for accounts that include access to the member CRM, Windows and MS Office 365, HR application, and any password managers.

Reg'd Association No: A0022649E
ARBN: 152 948680

5.6 Password security

- Staff must not exchange passwords under any circumstances.
- The password must be unique to ADAVB accounts that are not used outside the organisation.
- An ADAVB email ID and password must not be used for other personal accounts.
- Where staff need to write out passwords, they are obliged to keep the paper or digital document confidential in a locked physical storage location or an encrypted digital storage location and destroy it upon the cessation of their employment.
- Passwords must be changed at the direction of the Operations Manager when required. Generally, with a strong password and Multi-Factor Authentication, the need for password changes will be infrequent and in response to an identified threat, such as the appearance of the staff's, ex-staff's, and stakeholders' email addresses on the dark web.

6. DATA

ADAVB data is committed to robust and effective data storage and transmission control.

6.1 Data Sharing

ADAVB uses the internal server, MS Teams, and SharePoint to share documents securely with authorised staff and stakeholders.

- Sharing/transferring confidential data is not permitted unless authorised to do so.
- External applications (such as Conference apps) will use any ADVB data only after authorisation and a compliance and security check according to risk management best practices.
- Any sharing of confidential data must be done over the company network/ system and not over public Wi-Fi, private connection or USB drives.
- Member data should never be placed on a USB or portable hard drive.
- If member data needs to be shared with a third party (e.g., ADA or ADATas), it must be done using MS Teams/ SharePoint or a password-protected spreadsheet or document, with the password provided to the third party separately from the document.

6.2 Data storage

- Before storing or sharing confidential data, full-disk encryption will be enabled on work-supplied devices. Any "Bring your own devices" (BYOD) devices approved for use must also use full disk encryption.
- Outdated data will be deleted, and storage devices and drives will be zeroed using a digital file shredder tool.
- All physical and cloud backups, such as Outlook, Teams, and SharePoint files on portable drives, will be encrypted to prevent unauthorised access.
- Staff, external stakeholders and third parties are not permitted to download data onto a personal device and should use the association's internal server, Teams

Reg'd Association No: A0022649E
ARBN: 152 948680

and SharePoint environments. If data is downloaded to a personal device after permission is given it must be deleted as soon as possible after use. The third party must confirm in writing that the data has been deleted.

6.3 Data management

- ADAVB will periodically manage access and permissions and purge accounts, credentials, and permissions where necessary.
- Suspicious emails or attempted cyber-attacks to the Business Operations Manager to investigate and coordinate with the IT service Provider or other necessary parties.
- In the event of cyber incidents like scams, data breaches, or ransomware, report the occurrence immediately to the Business Operations Manager or, if they are unavailable, the IT vendor.
- ADAVB maintains a cyber security response plan that will be activated in the case of a reported data breach.

6.4 Documents and Meeting papers

- Document should, when practical, be sent to a Meeting papers should generally be provided to external stakeholders, committees and Council m as PDF documents. As a general principle, documents should be viewed in MS Teams and not downloaded to personal devices. If files are downloaded to a personal device to solve an access issue quickly, they should be deleted as soon as practicable, including from the Windows or other OS Trash Can.
- Due to the sensitivity and confidentiality of the Defence Committee, Disputes and Ethics Committee, and Honours and Awards Committee papers, they cannot be downloaded to personal devices. They must remain on ADAVB devices, defined as organisation-supplied computers and mobile equipment.

7. THEFT OR LOSS

- If a laptop, computer or mobile issued by ADAVB is stolen or lost, the matter and circumstances must be reported to the Business Operations Manager as soon as possible so that specific steps can be taken to secure data on the device.
- For insurance purposes, an incident report will be required to establish the circumstances of the loss or theft. In some cases, such as theft in a public place, a Police Report may need to be filed.
- A loss or theft, its circumstances, and the security mitigation steps taken will require the entry of the incident into the ADAVB's IT Risk register.

8. DEVICE USAGE

- Work devices (laptops and workstations) should be physically shut down at the end of each day or when not in use, except when the IT vendor or Business Operations Manager indicates that an application patch is scheduled.
- Work devices and mobile devices are set to lock the screen when not in use for longer than 15 minutes.
- Damage or conditions that prevent the device from working should be reported to the Business Operations Manager if IT support is unable to repair or restore

Reg'd Association No: A0022649E
ARBN: 152 948680

9. INTRUSION ATTEMPTS AND OTHER THREATS

There exist numerous motives and means for malicious actors to try to gain unauthorised as to a network, including data theft, ransom attempts, financial gain or to cause damage.

Common unauthorised intrusion attempts utilise hacking, exploiting vulnerabilities, or bypassing security controls, impersonating legitimate persons or entities through phone calls, emails or other communication channels, otherwise known as social engineering.

ADAVB maintains robust security measures such as firewalls, intrusion detection systems (IDS), spam filtering, white list access and regular security audits, along with continuously monitoring networks and systems for unusual or unauthorised activity.

Steps that members, staff and stakeholders can support the detection and prevention of intrusion attempts:

- Report any signs of potential attempts at intrusion or other malicious actions to the Business Operations Manager.
- Checking directly with a sender if the communication or document is genuine I there is reason to doubt
- Forwarding of suspicious email or other communications to the Business Operations Manager
- Carefully examine incoming mail from unknown sources or contacts.
- Be suspicious of attachments and links from the emails you receive, especially if they're from unknown contacts.
- Look for inconsistencies, grammar mistakes, spammy messaging, and promises.
- ADAVB maintains secure anti-spam, anti-malware and antivirus applications to flag spam, scam, and junk emails.

10. ADAVB WiFi

ADAVB may remotely monitor information transmitted over the internal network, Wi-Fi or VPN network to and from any other network device to ensure adherence to Branch Policies and to observe legal requirements. ADAVB will not access or monitor personal digital devices in any way.

11. DISCIPLINARY ACTIONS

Everyone, including our members, committees, stakeholders, and staff, requires complete confidence that their data is handled with care and security in mind. ADAVB, therefore, retains the right to take disciplinary action against staff who fail to follow security management protocols laid out in this policy.

The process of disciplinary action will follow the following levels of escalation:

- First-time, unintentional, small-scale security breach: ADAVB may issue a verbal warning and train the staff on security.
- For Intentional, repeated or large-scale breaches that cause severe financial or other damage, ADAVB will invoke more severe disciplinary action up to and including termination.

Reg'd Association No: A0022649E
ARBN: 152 948680

- Additionally, staff who are observed to disregard the ADAVB cyber security policy and or instructions may face progressive discipline, even if their behaviour hasn't resulted in a security breach.
- All disciplinary action is at the sole discretion of ADAVB.

Branch Policy Statement Number	**3.14**
Reviewed by Constitution and Policy Committee	**12 September 2024**
See also Related Branch Policy Statements	**BPS 1.05 Cyber Governance Policy** **BPS 1.08 Privacy** **ABPS 3.08 Use of Member Contact Details** **ABPS 3.09 Bring Your Own Device for ADAVB Business Use** **ABPS 4.03 Employee Disciplinary**

Appendix 1: Incident Response Plan

To be added

Reg'd Association No: A0022649E
ARBN: 152 948680