BRANCH POLICY STATEMENT 1.05

CYBER GOVERNANCE POLICY

1. INTRODUCTION

This Cyber Governance Policy establishes a framework for the secure management of digital assets within the ADAVB. It outlines the principles, roles and responsibilities necessary to protect sensitive data, comply with legal requirements, and mitigate cyber risks. It should be read with the ADAVB Branch IT and Data Security Framework.

2. SCOPE

This policy applies to all employees, members, contractors, third-party service providers, and other stakeholders involved in handling the organisation's digital assets, including hardware, software, data, and networks.

3. GOVERNANCE STRUCTURE

3.1. Council Oversight

The ADAVB Council oversees the cybersecurity strategy, ensuring that it aligns with the organisation's strategic objectives and that adequate resources are allocated for its implementation. Regular reporting to the Council on cybersecurity risks and incidents is mandatory, with an annual review of the Cyber Governance Policy and the IT and Data Security Framework.

3.2. Finance Risk and Audit Committee (FRAC)

FRAC will monitor the execution of the cybersecurity strategy as outlined in this policy and the IT and Data Security Framework. The committee is responsible for ensuring that cybersecurity risks are identified, assessed, and managed effectively. The committee will review the status of cybersecurity initiatives, incidents, and risk assessments.

3.3. Roles and Responsibilities

The ADAVB Business Operations Manager is responsible for developing, implementing, and maintaining the cybersecurity program. The Business Operations Manager will report on cybersecurity matters directly to the CEO and the ADAVB Council.

The ADAVB IT Service Provider manages cybersecurity measures, including monitoring and responding to threats.

The risk management team collaborates with the Business Operations Manager to identify and assess cybersecurity risks as part of the broader risk management framework.

All Employees must comply with cybersecurity policies and participate in training programs to understand their role in protecting the organisation's information assets.

4. CYBERSECURITY RISK MANAGEMENT

4.1. Risk Assessment

Regular cybersecurity risk assessments must be conducted to identify potential threats and vulnerabilities.

The results of these assessments should inform the prioritisation of cybersecurity initiatives and resource allocation.

4.2. Risk Mitigation

Implement appropriate technical, administrative, and physical controls to mitigate identified risks.

Continuous monitoring of the organisation's network and systems to promptly detect and respond to threats.

5. INCIDENT RESPONSE

5.1. Incident Reporting

All employees must immediately report cybersecurity incidents or suspicious activities to the Business Operations Manager, CEO or IT Service Provider.

An incident reporting mechanism should be available 24/7.

5.2. Incident Management

The ADAVB will maintain an Incident Response Plan (See IT and Data Security Framework) detailing the steps to be taken in the event of a cybersecurity incident.

The IRP includes communication protocols, roles and responsibilities, and containment, eradication, and recovery steps.

5.3. Post-Incident Review

After any significant cybersecurity incident, a post-incident review must be conducted to identify lessons learned and improve the organisation's cybersecurity posture.

6. COMPLIANCE AND AUDIT

Regular audits of cybersecurity controls and practices will be conducted to ensure compliance with the policy and relevant laws and regulations.

Any non-compliance must be reported to the CEO, and corrective actions must be taken promptly.

Branch Council shall receive regular reports regarding compliance with this policy.

7. TRAINING AND AWARENESS

All employees and volunteers must be provided with cybersecurity training as part of their onboarding process and participate in regular refresher courses.

The organisation will run ongoing awareness activities to educate employees about emerging threats and best practices.

8. DATA PROTECTION AND PRIVACY

Implement measures to protect sensitive data, including encryption, access controls, and data minimisation practices.

Ensure compliance with data protection laws and regulations outlined in the IT and Data Protection framework.

9. THIRD-PARTY RISK MANAGEMENT

Assess the cybersecurity practices of third-party IT Service Providers as part of the procurement process.

Include cybersecurity requirements in contracts with third parties, including provisions for incident reporting and data protection.

10. POLICY REVIEW

The Cyber Governance Policy will be reviewed annually or more frequently to ensure its effectiveness and alignment with the organisation's goals and the evolving cyber threat landscape.

Branch Policy Statement Number	**1.05**
Reviewed by Constitution & Policy Committee	**12 September 2024**
Adopted by Branch Council	**21 October 2024**
See also: IT and Data Security Framework	