Security and Technology Committee (STC) Charter

1. Introduction

This Security and Technology Committee (**STC**) Charter has been approved by the auDA Board (**the Board**). It sets out the role, responsibilities and procedures of the Security and Technology Committee (**the Committee**) and is consistent with rule 8.3 ('Terms of delegation') and 8.4 ('Proceedings of committees') of auDA's Constitution. It also supports the work of the Board of auDA Foundation Pty Ltd (**auDA Foundation Board**) as The Trustee for auDA Foundation. The auDA Board and auDA Foundation Board are collectively the auDA **Boards**.

2. Purpose

The Committee assists the auDA Boards to fulfil their governance and oversight responsibilities on matters relating to information, privacy, security, technology and business continuity.

3. Composition

3.1 The Committee will comprise at least three, but not more than five Board Directors.

3.2 The Chair of the Committee:

a) Must be appointed by the Board and

b) Must not be the Chair of the auDA Board or auDA Foundation Board.

3.3 The Board will review the membership of the Committee at least every two years, or as required.

4. Responsibilities

The Committee is responsible for the activities and other actions reasonably related to the Committee's purpose as may be assigned by the Board from time to time. The Committee will regularly monitor, review, provide guidance, seek assurance from Management and make recommendations to the Board on the following:

4.1 Internal controls

Internal policies and controls relating to information, privacy, cyber security, technology and risk.

4.2 Information Security, Data and Privacy

a) Policies and management systems for achieving compliance with privacy, data protection and information security legislation and other obligations

b) Regular reports received on privacy, including audits.

4.3 Risk management

a) Monitor risks related to the following risk domains and seek assurance from Management that they are within tolerance, and if not, confirm plans to bring them within tolerance:

- Cyber and Information Security risk domain
- Operational Resilience risk domain
- Technology and Innovation risk domain.

b) Advise the Finance and Audit Committee, at its next meeting via Management, of any changes to the risks domains at 4.3 (a) that have a material impact on auDA's Enterprise Risks.

c) Oversee an annual review of the Critical Infrastructure Risk Management Plan (**CIRMP**) required under the *Security of Critical Infrastructure Act 2018 (Cth).*

4.4 Security

a) Regularly monitor the integrity of auDA's security management against applicable policies and controls

b) Regularly monitor and review the security enforcing functions management has in place including:

- activity monitoring
- end-point protection software and processes
- vulnerability and/or penetration testing
- DDoS mitigation

to ensure they are fit for purpose and meeting the objectives of applicable security policies.

4.5 Technology

a) Oversee performance through the regular review of the Operational Resilience, and Technology and Innovation Key Risk Indicator Dashboard.

b) Monitor the governance and responsible adoption of emerging technologies, including artificial intelligence and quantum computing, ensuring that associated risks relating to security, privacy and regulatory compliance are appropriately identified and managed.

c) Oversee risks relating to critical system availability, performance and service continuity including monitoring significant outages or system failures ensuring appropriate remediation.

d) Monitor concentration risk and vendor dependency ensuring appropriate due diligence, contracting and vendor oversight

4.6 Business continuity

a) Regularly review Business Continuity planning and make recommendations to the Board as required

4.7 Monitor and regularly review the Incidence Response Policy and make recommendations to the Board as required.

4.8 Reporting

a) Maintain a matrix of material legislation with which auDA is required to comply Review draft annual reports prepared on security and risk issues in accordance with legislative requirements.

b) Review draft annual reports prepared on security risk issues in accordance with legislative requirements.

4.9 Other Responsibilities

a) Consider issues of relevance to auDA's security and technology and advise the Board as required.

b) Liaise with other Board Committees on those matters related to security and technology that are intrinsic to their roles, if necessary.

5. Terms

5.1 The Committee members shall be subject to the terms applicable under the Constitution of the Company.

6. Meetings of the Committee

6.1 The Committee is expected to meet at least four times per year, or as necessary to fulfil its role.

6.2 The quorum is minimum two members of the Committee.

6.3 The Committee may invite any person to attend all or part of a meeting of the Committee. The Board Chair and Directors may attend Committee meetings. The Chief Executive Officer, Chief Operating Officer, Chief Technology Officer, Chief Information Security Officer, General Counsel, and the Chief Financial and Risk Officer will be standing invitees and other senior members of the Company will be invited to attend as required.

6.4 Notice will be given to every member of the Committee, of every meeting of the Committee, at the member's advised email address for service of notice (or such other pre-notified interim address where relevant).

6.5 Committee papers will be distributed no later than seven (7) days prior to a meeting. Any papers distributed outside of this timeline will be at the Chair's discretion.

6.6 The Company Secretary will attend and support all Committee meetings.

6.7 The Company Secretary will prepare minutes of the Committee meeting, which shall be approved by the Chair of the Committee and circulated to members.

6.8 The Committee minutes shall be confirmed at the next meeting.

7. Administrative and operational support

7.1 The Company shall provide administrative and operational support necessary for the Committee to carry out its responsibilities.

7.2 All records, including the agenda and any reports or recommendations will be kept by the Company Secretary.

7.3 The Committee is entitled to rely on employees of the Company or professional advisers or consultants engaged by the Committee or the Company where:

- required to obtain a full appreciation of relevant issues
- there are reasonable grounds to believe that the employee, adviser or consultant is reliable and competent and
- the reliance was made in good faith and after making an independent assessment of the information.

7.4 The Committee may initiate special investigations and reports as it deems appropriate or as directed by the Board, in relation to matters contained in this Charter.

7.5 The Committee may obtain independent expert advice to assist in the discharge of its duties and obligations with such reasonable costs to be borne by auDA in alignment with the Company's Delegations Policy.

8. Review

8.1 This Charter has been endorsed by the Committee and approved by the Board.

8.2 The Committee will review its Charter once every two years and make recommendations to the Board as to any changes it considers should be made.

8.3 The Charter may be amended by resolution of the Board provided that any changes that would be inconsistent with the Company's constitution will require approval of the Company in general meeting to approve changes to the Company's constitution.

8.4 The Committee will undertake periodic self-assessments of performance.

8.5 The Board will review the Committee's performance at least once every two years.

9. Remuneration

9.1 Committee Members are entitled to reasonable expenses (including travelling and accommodation) incurred in carrying out duties as a Committee Member, in line with auDA's policies.

9.2 Each Committee Member is remunerated as part of their Remuneration as a Director, with the exception for the Chairperson, who is entitled to an additional annual fee (inclusive of superannuation) as determined by the Board.

10. Version Control

Next review: February 2027

Version	Change	Approval	Date
1	Original	Board	18 October 2019
2	Update	Board	7 April 2020
3	Update	Board	12 May 2021
4	Update	Board	6 June 2023
5	Administrative updates	Board	8 April 2025
6	Remove responsibility for enterprise risk and add technology	Board	23 June 2026