INFORMATION SECURITY MANAGEMENT POLICY STATEMENT

Toustone achieved ISO27001:2022 certification in December of 2023.

Toustone follows the principles of the Australian Cyber Security Centre - Govern, Protect, Detect and Respond.

- Govern: Identifying and managing security risks.
- Protect: Implementing controls to reduce security risks.
- Detect: Detecting and understanding cybersecurity events to identify cybersecurity incidents.
- Respond: Responding to and recovering from cyber security incidents.

Information Security Management System

Toustone's Information Security Management System (ISMS) has been implemented to safeguard the organisation's information assets from threats posed by threat actors and other vulnerabilities.

ISMS encompasses Toustone's operations, spanning design, development, maintenance, data management, technical support, sales and marketing, HR, and Finance to Toustone's Statement of Applicability dated 15 May 2023.

Information Security Objectives

Toustone aligns it's information security to four objectives. These are:

Objective One:	Ensure the confidentiality, integrity, and availability of the organisation's information assets.
Objective Two:	Protect information assets against unauthorised access, disclosure, modification, destruction, or interference.
Objective Three:	Ensure compliance with regulatory, legal, and contractual requirements related to information security.
Objective Four:	Establish a culture of security awareness and responsibility among all staff and stakeholders.

Metrics and reports designed to monitor the ISMS and its operational effectiveness have been developed for each of the 4 security objectives and are provided for Board review each quarter.

Governance

The ISMS operates under the governance of the Information Security Steering Committee (ISSC), which meets regularly to review the system's effectiveness, set strategic directions, and address significant risks. The ISSC is also responsible for planning of changes, resources and ensuring those working on the ISMS have the right competence.

Awareness & Communication

Awareness and communication of the ISMS is promoted via Toustone's security awareness program. Awareness and communication includes:

- Implementation of controls.
- Reminders of policies and procedures.
- General security awareness.

Policy Framework

Complimentary to the ISMS is a comprehensive Information Security Policy Framework including:

- Organisational Controls
    - Information Security Policy
    - Cybersecurity Incident and Data Breach Management Policy
    - Information Security Rick Management Policy and Procedure
    - Supplier Management Policy and Procedure
    - Audit and Corrective Actions Policy and Procedure
    - Data Lifecycle Policy
    - Business Continuity Plan
    - Information Security Risk Register
    - Supplier and Information Asset Register
- People Controls
    - Acceptable Use Policy
    - Information Security for Human Resources Policy and Procedure
- ICT Controls
    - Access Control Policy and Procedure
    - Change Management Policy
    - Secure Development Policy
    - ICT Cybersecurity Policy
    - Patch and Vulnerability Management Policy