1. Purpose

This top-level Policy provides the direction, scope and approach to information security within Toshiba (Australia) Pty Ltd's working environment.

The overarching objective of this Policy is to protect information assets - which create, process, store, view or transmit information - against unauthorised use or accidental modification, loss or release.

2. Scope

This Policy applies to the entire Information Security Management System (ISMS), as defined in the ISMS Scope Document.

All staff, users, and external parties who have access to Toshiba (Australia) Pty Ltd's information assets are required to comply with this Policy and any supporting systems, policies, procedures, codes of conduct, or related obligations.

3. Policy Statement

Toshiba (Australia) Pty Ltd (**TAP**) is committed to information security and the management of risks associated with information within our organisation. We recognise the importance of information as a valuable asset to our business, customers and other stakeholders which requires protection against misuse.

TAP's support for this Policy and our commitment to ensuring information security is achieved by:

- Allocating the resources necessary to support this Policy and objectives.
- Maintaining an Information Security Management System which meets the requirements of ISO 27001:2013.
- Establishing information security controls based on internationally recognised best practice.
- Adopting a framework for setting information security objectives.
- Complying with applicable legal, regulatory, contractual and other requirements related to information security.
- Continually improving the effectiveness of our Information Security Management System.

TAP endorse this Policy through the leadership and commitment of our Top Management who provide the strategic direction and resources needed to maintain and improve our information security practices.

It is only through a collective commitment from TAP management, staff and external parties that we are able to ensure protection of our information assets.

4. Information Security Objectives

In addition to the overarching objectives of this Policy, TAP has implemented a framework for setting information security objectives across relevant functions and levels of our organisation.

The key information security objectives of Top Management in implementing the information security management system are:

- Ensure the confidentiality of our information assets are protected and maintained
- Ensure the availability of our information assets are protected and maintained
- Ensure the integrity of our information assets are protected and maintained
- Ensure that our organisation and people are able to systematically manage and maintain information security within our business
- Provide customers with the assurance that information security is recognised as an integral part of our business through our certification of the information security management system

Information Security Objectives are established, planned and documented as part of TAP's management review process. Planning includes defining actions, allocating resources and responsibilities, and setting agreed time-frames for monitoring, completion and evaluation of results.

5. Communication

TAP ensures this staff, users and relevant external parties are made aware of this Policy through suitable methods of communication.

Any questions regarding this Policy should be directed to TAP's Information Security Manager.

6. Discipline

Failure to comply with the terms of this Policy may result in disciplinary action. Staff disciplinary processes are specified in TAP's *Staff Code of Conduct Policy.* Employee discipline is determined by TAP Policy and procedure and employment contracts, as applicable.

Conduct in contravention of this Policy may also result in an offence or crime under relevant State and Commonwealth legislation, resulting in prosecution. Where a violation is considered a criminal offence, the police (Federal and State) will be informed.

TAP's Human Resources department will manage disciplinary and related matters.

7. Review

The Information Security Manager, or their delegate, is responsible for the review of this Policy. The Policy shall be reviewed at least once annually in accordance with TAP's procedure *Document and Record Control*.

Bret Davies
Managing Director
Toshiba (Australia) Pty Ltd

4 November 2022