Digital Trust Program

BITS Technology Group Pty Ltd

Action	Name	Title
Prepared By	Muhammad Nauman Mustafa	Cyber Security Engineer
Reviewed By	Blair Munro	Head of Technology
Approved By	Bernard Mangelsdorf	Chief Executive Officer

Version	Date	Description of Change	Updated By
1.0	12 March 2025	Initial Policy Creation	Muhammad

1. Purpose

This policy establishes criteria for classifying suppliers based on their cybersecurity posture and data handling practices to ensure the protection of organizational assets and compliance with regulatory requirements.

2. Scope

Applies to all third-party suppliers, vendors, and service providers who interact with, process, or store organizational data.

3. Trusted Supplier Criteria

A supplier will be classified as Trusted if they hold at least one of the following certifications or compliance frameworks:

- ISO/IEC 27001 Certification
- SOC 2 Certification
- Compliance with the Australian Privacy Principles (APPs)
- General Data Protection Regulation (GDPR) Compliance

Trusted suppliers are presumed to have adequate cybersecurity and privacy controls in place.

4. Conditional Trust Classification

Suppliers without the above certifications will be further assessed based on their access to critical or sensitive data, including but not limited to:

- Personally Identifiable Information (PII)
- Financial data
- Intellectual property
- System credentials or access to internal infrastructure

If such data is involved, the supplier must:

- Provide a documented summary of their cybersecurity and privacy practices.
- Include security measures in their publicly available privacy policy or upon request.
- Agree to the organization's Digital Trust Agreement outlining minimum cyber hygiene requirements and incident notification obligations.

5. Non-Trusted Suppliers

Suppliers who:

- Do not hold recognized certifications, **or**
- Do not handle critical or sensitive data

are not required to meet trust classification requirements but must still adhere to basic contractual obligations and data protection clauses.

7. Compliance

Supplier classifications will be reviewed annually or upon significant changes in service scope and the organization reserves the right to audit or request updated documentation at any time.