

Supplier Information Security Policy

Titomic Limited is pioneering alternative, advanced and sustainable manufacturing solutions for the global market including traditional metal-based industries. We aim to maintain market leadership by contributing to our customers' success.

Integral to our Information Technology and Cybersecurity (ITCS) Management System, is managing risk; encouraging risk-based thinking supported by the Physical, Logical (Technical) and Behavioural access controls implemented to prevent data and IP theft, blocking scams and security breaches.

Titomic has implemented information security measures to detect and rapidly respond to incidents, ensuring confidential information remains secure, backed-up, mitigating potential detrimental impact on Titomic's systems, website, software access and business operability. Titomic's technology infrastructure, IP and reputation are protected through the sophisticated use of ABAC (Attribute Based Access Control) and MFA (Multifactor Authentication).

Expectation of Suppliers to Titomic:

Engagement with suppliers may be dependent on cyber security authorisation.

Titomic's Cyber security team may request evidence of the following items below:

- Evidence of Accreditations, including SOC 2, ISO27001, ISO27002, and for cloud services compliance to ISO27017 and ISO27018.
- Evidence of the implementation and compliance to SSDLC (Secure Software Development Lifecycle) methodology.
- Relevant government or industry licence / accreditation / certification
- Compliance to geographical legal frameworks and protection of data.
- Disclosure of 3rd Party collaboration
- Disclosure of location of data centres
- Disclosure of roll back and backup restoration policy and test plans
- MFA enabled RMM / PSA Technology
- Application Controls optimised
- Patching regime across, operating systems, networks and systems reducing risk of software vulnerabilities being exploited.
- Restriction of administration privileges
- Delivery of Service Level Agreement terms
- Certificate of Currency Products Liability insurance
- Satisfactory completion of SCM-010 Supplier Security Questionnaire
- Other documentation requested by Titomic's cyber security team.

Commitment to delivering value to Titomic:

- Confirmation of Cybersecurity roles including the scope of leadership and ownership within your organisation
- Confirmation of commitment to ongoing training and awareness briefings for staff
- Incident response management and communication to Titomic of impact on data security.
- Managed update process including proactive testing with the Titomic team to ensure debugging within a sandboxed instance and User Acceptance Testing prior to go live for new installations and subsequent updates of customised solutions.
- Rigorous monitoring is undertaken by Titomic, and regular reporting may be requested for validation of security posture assessments.
- Commitment to communicate regularly with Titomic about changes within your ownership, security posture and lifecycle of service or product provided to Titomic.
- Commitment to work with Titomic as we strive to exceed our customers' expectations by ensuring data security, confidentiality and staff act to fulfil their individual responsibilities to the Titomic ITCS Management System.