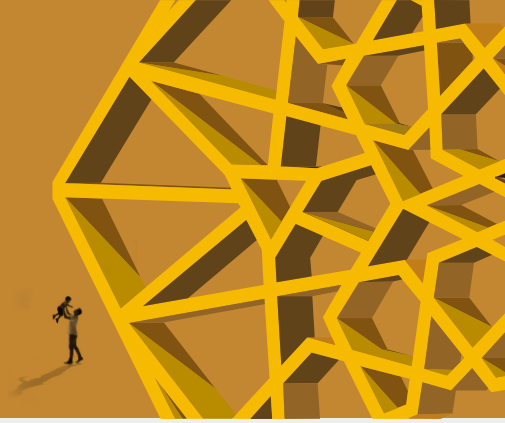
IS MANAGEMENT SYSTEM POLICY



Zutari provides engineering, management, specialist technical and advisory services for government and private sector clients globally. As an engineering and advisory organisation, information is central to everything we deliver. It is therefore critical that the information assets of the organisation, our clients, and our partners are properly managed and protected.

To ensure this, Zutari is committed to maintaining an Information Security Management System (ISMS) aligned with the requirements of ISO 27001, applicable to all employees and third parties who access or handle Zutari or client information in any form. This reflects our recognition that information security is fundamental to client trust, operational integrity, and our obligations under applicable data protection and privacy legislation across the jurisdictions in which we operate.

Zutari's executive management provides active leadership and commitment to the ISMS and is ultimately accountable for its effectiveness. They also ensure that sufficient resources are made available to support the ISMS operation and its continual improvement. The day-to-day operation and maintenance of the ISMS is performed by a dedicated IT services team.

The ISMS is built on a risk-based approach designed to protect the confidentiality, integrity, and availability of information across operations. Organisational, people, physical and technical controls are implemented and maintained across the areas listed below, in line with identified risks and the applicable information security domains:

ISMS governance and control review - key ISMS documents and control activities are reviewed within defined timeframes to ensure continued suitability, adequacy, and effectiveness.

Awareness and training - employees and relevant third parties are made aware of their information security responsibilities through defined awareness and training initiatives, supporting consistent understanding and application of information security practices across the organisation.

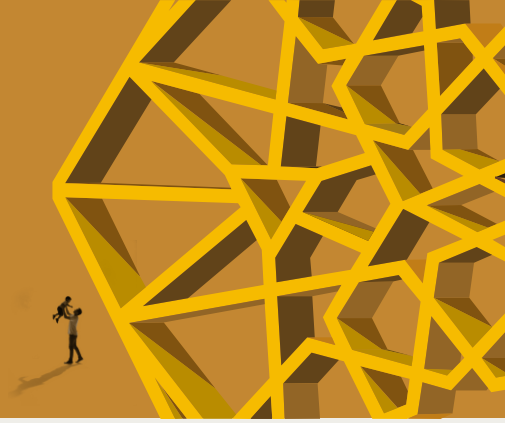
Regulatory and contractual compliance - applicable legal, regulatory and contractual information security obligations are identified, assigned ownership, and tracked to remediation, with periodic review of compliance across jurisdictions.

Access control and identity governance - access to systems and information assets is granted, reviewed, and revoked in line with documented procedures and defined business requirements.

Data protection - information is progressively classified and labelled in line with defined standards, and protected throughout its lifecycle, including creation, processing, storage, transmission, archiving and secure disposal. Appropriate controls are applied across key platforms and relevant areas to reduce the risk of unauthorised disclosure, with retention and controlled archiving ensuring that information is maintained for defined business purposes and not retained longer than necessary.

ZUTARI

IS MANAGEMENT SYSTEM POLICY



People security – Employees with access to Zutari systems or data are vetted prior to onboarding and re-vetted on material role changes, and are bound by the Conditions of Employment throughout their tenure.

Supplier and third-party security - third parties with access to Zutari systems or data are subject to defined security assessment prior to onboarding, and their risk is reviewed at planned intervals based on criticality, exposure and role change.

AI and emerging technology governance - AI tools and emerging technologies are subject to risk assessments and approval prior to use, with appropriate controls applied to manage information security and data handling risks.

Incident response readiness - defined processes exist for the detection, triage, response, and post-incident review of information security incidents, with lessons learnt applied to strengthen controls and reduce recurrence.

Business continuity and recovery - recovery objectives are defined for critical systems, and business continuity and disaster recovery plans are maintained, reviewed, and tested at planned intervals.

Zutari maintains formal information security governance with clearly defined accountability at leadership, operational, and user levels. All personnel and third parties with access to Zutari's information systems are required to comply with information security requirements, and non-compliance may result in disciplinary action, up to and including termination of employment for employees and termination of contract for third parties.

> The effectiveness of the ISMS is measured through regular monitoring and reporting of information security performance to executive leadership, with objectives established and operationalised, and controls reviewed against business needs, risk exposure, and the evolving threat landscape. Zutari is committed to the continual improvement of the ISMS, using lessons learnt from incidents, audits, and reviews to strengthen information security practices over time.

Teddy Daka
GROUP CHIEF EXECUTIVE OFFICER

DOC NUMBER: PLY-IT-00016

Date: August 2026