Information Security Policy

Joss recognises that the security of information, and the systems that store, process and transmit it, is fundamental to the protection of our business, our clients and the people we work with.

Joss operates across the construction, facility management, and cleaning industries for a broad range of government and private clients. The information we hold includes client and contract data, personal information, financial records and commercially sensitive material. Protecting this information is an obligation to our clients, our employees and the community.

The purpose of this policy is to preserve the confidentiality, integrity and availability of the information Joss holds. It sets out the Company's commitment to managing information security risk through a structured Information Security Management System (ISMS).

Policy statement

It is the Company's policy to maintain an ISMS that complies with the requirements of ISO/IEC 27001 and to fulfil the following commitments:

- Establishing and maintaining an ISMS that identifies information security risks, implements appropriate controls, and monitors their effectiveness on a continuous basis;
- Setting measurable information security objectives and reviewing these annually to ensure ongoing improvement in the protection of Company information assets;
- Classifying information assets according to their value, sensitivity and criticality, and applying controls commensurate with that classification;
- Controlling access to information systems and data so that only authorised individuals can access information relevant to their role;
- Ensuring all personnel, including employees and subcontractor workers, understand their responsibilities for information security through appropriate induction, training and awareness programs;
- Implementing physical and technical controls to protect information assets from unauthorised access, disclosure, modification, destruction or interference;
- Managing information security obligations in supplier and subcontractor relationships through contractual requirements and periodic review;
- Complying with all applicable legislative and regulatory requirements and any client-specific information security obligations under Commonwealth and State Government contracts;
- Establishing and maintaining an information security incident management process to enable timely detection, reporting, containment and recovery; and
- Continually improving the ISMS through internal audit, management review, and the systematic treatment of identified risks and non-conformances.

Joss will meet these commitments by providing the necessary resources and maintaining documented procedures that comply with or exceed the requirements of ISO/IEC 27001, the Australian Privacy Principles and any applicable Commonwealth and State Government information security requirements.

Scope

This policy applies to all Joss workers, information assets and systems within the boundary of the ISMS, as defined in the ISMS Scope Statement. It extends to subcontractor workers who access Company information or systems.

Responsibilities

Accountability for the ISMS rests with top management. The Chief Executive Officer is the ISMS Owner and holds overall accountability and authority for the ISMS, including ensuring it is established, maintained and continually improved in line with ISO/IEC 27001:2022, providing the resources it requires, approving the Statement of Applicability (SoA) and Risk Treatment Plan, and acting as the final risk-acceptance authority for risks rated High or Extreme. The Chief Executive Officer assigns operational responsibility for the ISMS to the ISMS Manager, who ensures the ISMS conforms to the standard and reports on its performance to top management. Responsibility for implementing and operating the technical controls within the ISMS rests with the ISMS Implementation Lead. These roles are summarised below.

Role	Holder	Information security responsibility
ISMS Owner (top management)	Chief Executive Officer	Overall accountability and authority for the ISMS; provides resources; approves the SoA and Risk Treatment Plan; final risk-acceptance authority for risks rated High or Extreme; chairs the management review.
ISMS Manager (management representative)	GM Risk and Compliance	Day-to-day operational ownership of the ISMS; maintains the Risk Register, SoA and Risk Treatment Plan; drives risk treatment to closure; ensures the ISMS conforms to ISO/IEC 27001:2022; reports ISMS performance to top management at each management review. Independent of the implementation of the technical controls.
ISMS Implementation Lead (technical control owner)	IT Manager	Implements and operates the technical and secure-development controls; supports risk assessment and treatment; reports control status and incidents to the ISMS Manager. Does not self-approve the adequacy of the controls they implement.
All workers	Employees, subcontractors and labour hire workers	Protect information assets; comply with this policy and supporting procedures; report any actual or suspected incident, breach or vulnerability to the ISMS Manager without delay.

6th July 2026

Edward Whiting
Chief Executive Officer