ELMO

Security Statement & Assurance Overview

At ELMO Software, we understand that our products play a key role in helping our customers manage their most important resources, their people. Our customers trust us with their employee information and we take this responsibility seriously.

This document provides an overview of ELMO's information security, governance framework, technical control environment, privacy, resilience measures, identity and access controls, and customer assurance approaches before more sensitive evidence is considered for controlled release.

Previously issued as the Information Security Statement, this version document 2.0 is now titled Security Statement and Assurance Overview.

Assurance Framework

ELMO's information security is supported by formal governance, technical controls, independent assurance activities, and a controlled evidence release process for deeper customer diligence.

Your trust. Our priority

ELMO is built on a foundation of security, privacy, and responsible AI. We are committed to protecting your data and delivering dependable, compliant solutions.

Security

Enterprise-grade security across our platform • Encryption in transit and at rest • Continuous monitoring and threat detection • Regular third-party penetration testing

Privacy

Privacy by design and default • Data minimization and purpose limitation • Strict access controls and least privilege • No sale of your personal data

Compliance

Aligned with leading industry standards • SOC 2 Type II compliant • ISO/IEC 27001:2022 certified • Ongoing audits and compliance reviews

AI Assurance

Responsible AI principles at our core • Human oversight and model accountability • ISO/IEC 42001:2023 certified • Transparency in AI functionality and use

ELMO is committed to earning and maintaining your trust—today and every day.
Secure. Private. Compliant. Responsible.

Security Governance and Certification

We maintain an information security management framework that meets industry standards and customer assurance expectations.

We're ISO/IEC 27001:2022 certified and also align our broader assurance with SOC 2 Trust Service Criteria and the Australian Cyber Security Centre Essential Eight.

We maintain a security-first mindset supported by employee awareness obligations and engineering practices informed by secure coding principles and recognised threat and vulnerability knowledge sets, including OWASP and MITRE ATT&CK.

Our security framework is supported by documented plans and procedures covering incident response, data breach response, supplier governance, operational monitoring, and resilience.

Security responsibilities are embedded across business functions so that employees understand the role they play in protecting customer and corporate information.

Information Security Policy Outcomes

ELMO maintains an established information security policy and supporting procedures aligned to the ISO/IEC 27001 management framework.

- Information is accessible only to authorised people inside or outside ELMO, according to business need.
- The confidentiality, integrity, and availability of information and systems are protected through defined controls and governance practices.
- User responsibilities and obligations for protecting corporate information and systems are identified, communicated, and managed.
- Employees receive information security training and are informed that compliance with security requirements is mandatory.
- Supporting procedures exist across areas including malware protection, password management, incident response, and business continuity.
- The framework supports protection against business damage, legal liability, and the inappropriate use of information and systems.
- Legal, statutory, regulatory, contractual, and business requirements are incorporated into the operation of the information security framework.

Security Roles and Responsibilities

Our security responsibilities are supported by roles across information security, platform and infrastructure engineering, and information security consulting functions. These roles work together to ensure security is embedded across business functions, operational decision-making, and customer assurance activities.

This includes leadership and oversight responsibilities performed by the Head of Information Security, platform and infrastructure engineering leadership, and information security consulting roles.

Technical Security Control Environment

PLATFORM AND INFRASTRUCTURE SECURITY

We apply a layered, defence-in-depth security model across its environment, including network segmentation, vulnerability management, penetration testing, encryption, and continuous monitoring.

ELMO's hosted application architecture operates within secure AWS-based virtual private cloud environments using security groups, network access control lists, and flow logging to support network protection and traffic visibility.

Customer data is encrypted at rest using AES-256 and encrypted in transit using SSL/TLS. Encrypted backups and secured transfer methods such as HTTPS and SFTP are used to protect data throughout its lifecycle.

SECURITY ENGINEERING PRINCIPLES

We apply secure engineering principles across the design, development, deployment, and operation of our systems and services.

- Secure coding practices are used throughout software development, supported by peer review, testing disciplines, and security tooling intended to reduce the risk of vulnerabilities reaching production environments.
- Systems are designed using separation of concerns and defence-in-depth principles so that distinct security layers work together to reduce the likelihood and impact of control failure.
- Applications and systems follow least-privilege and need-to-know access principles, supported by strong authentication and session management controls.
- Technical information that could assist attackers is restricted in production environments, including the disabling of user-accessible debugging functionality.
- Dependencies on third-party systems and services are subject to review, tracking, minimisation where practical, and ongoing security assessment so that supporting services maintain an appropriate security standard.
- New technologies and architectural designs are reviewed and approved before adoption to manage change-related security risk.

- Legacy or unsupported technologies are reviewed and replaced prior to end-of-life where required to maintain security supportability and patching coverage.
- Sensitive information in transit and at rest is protected through encryption controls, and personal information handling is supported by monitoring, alerting, and reporting mechanisms that assist security and compliance oversight.

IDENTITY AND AUTHENTICATION

Identity and access security is an important part of ELMO's control environment for both customer-facing products and internal operations.

Across the product environment, ELMO supports identity and authentication controls that are commonly requested during customer diligence, including single sign-on capability, identity provider integration, role-based access controls, multi-factor authentication for privileged access, and audit logging of relevant access-related activity.

For internal operations, multi-factor authentication is enforced across privileged accounts, and VPN-based remote access with two-factor authentication is used where remote connectivity is required.

AUTHORISATION AND ACCESS MANAGEMENT

Access to systems and data is governed through role-based and least-privilege principles designed to align user access with business needs.

ELMO also uses strong password controls, notifications of multiple login failures, account operation logging, and server-side IP restrictions to reduce brute-force and unauthorised access risk.

Privileged access is subject to tighter control measures than standard user access, reflecting the elevated risk associated with administrative permissions.

SECURITY TESTING AND VULNERABILITY MANAGEMENT

ELMO performs regular vulnerability testing and annual independent penetration testing as part of its assurance program.

This annual independent testing covers all client-facing cloud products and also extends to critical infrastructure and supporting environments that are material to service security.

The objective of this testing program is to identify and remediate security weaknesses through an externally validated process rather than relying only on internal assurance activity.

MONITORING, DETECTION, AND INCIDENT MANAGEMENT

Central monitoring is placed across environments and applications, with alerts distributed through operational channels that support continuity of visibility and response.

ELMO supports systems on a 24/7 basis and uses multiple incident alerting channels together with defined response roles to support timely triage and resolution.

We maintain documented incident response and data breach response plans aligned to recognised frameworks and established response practices.

Customer communication occurs once the nature and impact of an incident has been determined, and post-incident review forms part of the formal response process

Privacy and Data Protection

ELMO is committed to protecting personal data in line with applicable privacy obligations, including the Australian Privacy Principles, the Privacy Act 1988, and relevant international privacy requirements.

Privacy practices include privacy-by-design measures, support for data subject rights, transparency around personal information handling, secure deletion, and privacy training for employees handling customer data.

Privacy obligations are supported by documented policies and response plans, including privacy management, information security, and data breach response procedures.

ELMO also maintains a program for data classification and protection, together with controls addressing the use, disclosure, protection, retention, and destruction of sensitive information.

As a SaaS provider, we're responsible for the secure handling, storage, and transfer of customer data, and work with customers to support an appropriate understanding of their responsibilities when configuring access controls and using the platform.

Hosting, Backup, and Resilience

ELMO hosts customer data in Australia and aligns data sovereignty and residency to Australia. Backup arrangements include daily backups retained for defined operational periods and longer-term archival retention to support resilience, recovery, and evidentiary needs.

Disaster recovery measures include backups stored in a separate disaster recovery environment, recovery testing, multi-availability-zone hosting, infrastructure-as-code restoration practices, and defined recovery targets. Business continuity and disaster recovery testing is conducted on a recurring basis, and formal recovery objectives are defined and tested.

Supplier and Third-Party Governance

Supplier agreements include information security requirements, and due diligence with risk analysis is undertaken before supplier engagement.

ELMO maintains a central supplier management process and performs periodic risk review activity across relevant supplier relationships.

ELMO also operates a subprocessors management framework, with due diligence and contract review controls applied to relevant third-party providers.

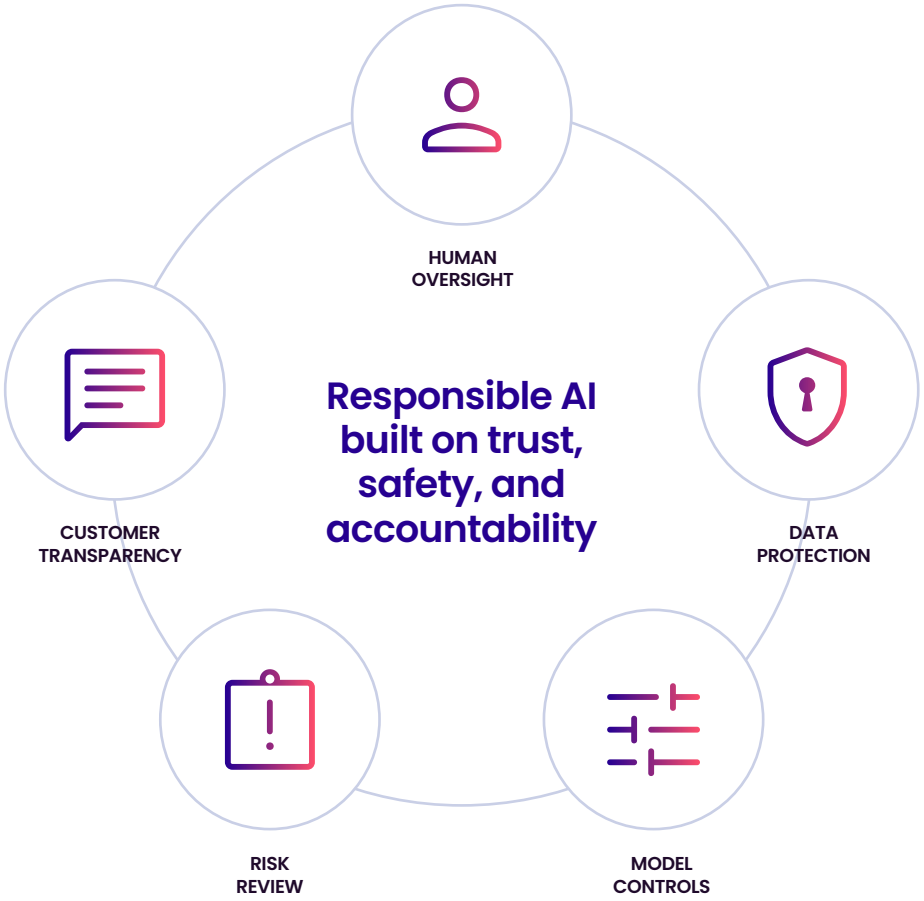
AI Assurance Position

ELMO's AI assurance approach is designed to support trust, governance, and responsible use of AI-enabled capabilities across the platform.

We're certified to ISO/IEC 42001 and its Artificial Intelligence Management System operates alongside the existing ISO/IEC 27001 information security framework, and apply a human-in-the-loop philosophy so that AI augments decision-making rather than autonomously determining critical HR outcomes.

Customer data used in AI-enabled services is logically separated, encrypted in transit and at rest, hosted in Australian AWS environments, and not used to train public models.

We recognise that customers increasingly seek clarity on where AI is used, how data is handled, whether AI functionality is optional, and what safeguards are in place. This assurance approach is intended to provide that additional transparency.



Customer Assurance and Evidence Release

ELMO provides assurance information in stages, beginning with summary material and moving to controlled evidence where deeper diligence is required. Additional supporting documents may be shared under controlled conditions, including NDA where appropriate. Where detailed reports are sensitive or proprietary, attestation-based evidence may be provided instead.