Information Security Statement

At ELMO we understand that our Cloud HR & Payroll 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.

We use ***secure engineering principles*** to build services, architecture, software and systems. Security principles are designed into our software systems from the earliest development opportunity. These principles are:

- **Secure Coding:** Developers use secure coding practices and techniques, including pair programming, refactoring, defence in depth, separation of concerns, peer review and test-driven development. Automation frameworks for development and software release utilise security tools that scan for vulnerabilities using quality gates so that no vulnerabilities can be released into the production environment.
- **Separation of Concerns**: Systems in different security domains or levels of trust are logically kept separate from each other by security controls that prevent lateral movement to a higher security domains or levels of trust without appropriate authentication and authorisation.
- **Defence in Depth**: No one security control is solely responsible for preventing unauthorised access or protecting against the exploitation of vulnerabilities. This requires overlapping coverage of security controls by distinct layers or components within a system. An example of this would be the usage of a WAF (Web Application Firewall) in front of a website, which in and of itself contains protections against injection attacks. This guards against any one layer or component failing 'open' and thereby leaving a system vulnerable to attack.
- **Silent Running**: All applications and systems avoid giving away technical information about their implementation that an attacker could use to their advantage. In particular user accessible technical debugging controls are completely disabled in the production environment.
- **Access Control**: Systems are designed to follow least privilege and need-to-know principles when controlling access to services and information they contain. Further appropriately strong authentication and session management mechanisms are implemented.
- **Management of Dependencies**: Systems often depend upon other systems or services to implement their functionality. ELMO requires the other systems or services to be equally as secure as the core system. This requires a structured approach to dependency analysis, tracking and dependency minimisation combined with regular security reviews and screening for such dependencies. Ideally automated screening is utilised where possible. Only prior security reviewed and approved vendors are used.
- **New Technologies and Architectural Designs**: Change can introduce security risks, for systems this most often occurs when using new technologies or new architectures. To manage this risk new technologies and architectural designs must undergo review and approval.
- **No Longer Supported (End of Life) Technologies**: The usage of legacy or retired technologies that do not have an ongoing security support or patch regime create a serious security risk, in that an exploit could be discovered which is never going to be addressed. Such technologies used in our systems or services are either removed or replaced prior to End-of-Life. Technologies in use are regularly reviewed, every 6 months at least, to plan for their advance replacement.
- **Encryption**: Sensitive information in transit and at rest is always encrypted in accordance with the Cryptography Procedure.
- **Supporting Privacy Principles**: Personal Information is appropriately secured and its usage tracked and monitored. Alerting and reporting are implemented to allow security and regulatory compliance oversight.

The ***security of information is a core pillar*** of the products and services we deliver. We manage our privacy obligations to ensure the confidentiality, integrity and availability of information is in line with Australian and New Zealand Privacy legislation as well as GDPR. As a SaaS provider ELMO's responsibility covers the secure handling, storage and transfer of our client's data. ELMO works closely with clients to ensure they understand their responsibilities to ensure they set the appropriate access control models so the right users have the

right access to their HR and Payroll data. This ensures that clients can meet their own legislative and regulatory data privacy requirements.

Maintaining ***best-of-breed security competencies*** is one of our information security objectives. With the increasing regulatory and operational requirements to ensure personal information is kept secure against sophisticated attacks, ELMO systems are built with a security-first mindset. Key to this is engineers having a grounding in secure coding principals and techniques, 'know thy enemy' training consisting of understanding both the most common website vulnerabilities (OWASP) and the ways in which an attack can progress through a system to extract information (MITRE ATT&CK). This knowledge enables our engineers to code and develop highly secured systems on an ongoing basis. Additionally, all ELMO employees are required to have a firm understanding of information security in line with our Information Security Policy.

ELMO has an established and well-embedded ***Information Security Policy***. The purpose of this policy is to establish the framework to ensure information security management is managed in accordance with ISO/IEC 27001 and achieves the following:

- Information is accessible only to authorised persons inside or outside ELMO
- Ensures the confidentiality, integrity and availability of information and systems
- Identifies, communicates and manages the responsibilities of users and their obligations to help protect corporate information and systems
- All users are trained on information security and are informed that compliance with this policy is mandatory
- Procedures exist to support information security policies – including, but not limited to malware protection, password management and business continuity management
- Protects ELMO from business damage or legal liability and the inappropriate use of ELMO information and systems
- Meets country, state and territory legal, statutory, regulatory, contractual and business requirements.

ELMO maintains ***strong relationships with suppliers***. Our key suppliers have been selected for the breadth and depth of their security credentials. But all of our suppliers are important to us, each undergoes proper due diligence and thorough vetting prior to engagement including a risk analysis prior to establishing a formal relationship.

As a SaaS provider, ***uninterrupted access to our systems*** is codified in our availability service level of 99.5% uptime. We achieve this in a number of ways, our infrastructure incorporates both resiliency and redundancy, our software development lifecycle is strictly controlled and managed, backup and restore procedures are tested on a regular basis.

ELMO's dedicated Security Team includes Carmen Nunez and Grazia Lucisano. Together they ensure that security is embedded across all business functions and that all employees consider security in the context of their roles and the customer impact. Their unique blend of experience and skills enables them to keep ELMO and our customers secure in an evolving threat landscape.

Carmen Nunez is ELMO's Senior Information Security Manager and a risk, governance and compliance expert. Since 2018, she has managed ELMO's multiple ISO 27001 certifications. She is a Certified Information Privacy Manager (CIPM) and an IRCA Certified ISMS Associate Auditor.

Grazia Lucisano is ELMO's Information Security Consultant. She is an HR and recruitment specialist who joined ELMO's Talent Acquisition Team in 2019, transitioning to the ELMO Security Team in March 2022. She has a Law degree from the University of Bologna Italy, is a Certified Information Privacy Manager (CIPM) and a Certified ISO 27001 Internal Auditor.

ELMO has been certified to ISO 27001 since 8 July 2019 and transitioned to ISO 27001:2022 in December 2023.