ELMO's approach to vulnerability management

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.

Security is a 24/7 concern and requires a broad set of tools and methodologies working together to provide resilient services. At ELMO security is considered at multiple levels, from the initial web request all the way through our systems to how customer data is stored. Underpinning this a focus on policy-based security controls operating within an Information Security Management System (ISMS) framework.

ELMO utilises world class data centres such as AWS Australia and Microsoft Azure, taking advantage of the latest technologies, to ensure our applications and customer data remain secure and available.

As part of our Software Development Life Cycle ELMO employs code level scanning to determine vulnerabilities to be remediated as part of the release process. Automated scanning tools are utilised as well as automated vulnerability scanning.

In addition, annual penetration is conducted on all applications. ELMO engages an independent penetration test vendor to complete vulnerability assessments of all ELMO Group applications.

ELMO is happy to share further details of these independent assessments to provide customers with assurance that our processes and systems are secure (note - provision of these reports may be subject to appropriate controls such as signing an NDA).

ELMO does not permit the following types of security testing:

To safeguard our customers, vulnerability testing is always conducted using specially provisioned test sites (replica of production, but completely segregated). This ensures vulnerability testing cannot disrupt the service we provide to our customers.

Vulnerability testing must NEVER be performed on ELMO production sites.

ELMO treats unauthorised attempts to access our applications and/or infrastructure as extremely serious, as they can impact the integrity of service and operational performance for all customers. The following are expressly prohibited:

- Performing actions that may negatively affect ELMO or its users (e.g. Spam, Brute Force, Denial of Service…)
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you
- Introduction of 'malware' or other attacks that may cause loss of system or application integrity or disclosure of data from systems and services
- Conducting any kind of electronic attack on ELMO personnel, property or data centers
- Social engineering any ELMO employee or contractor
- Conduct vulnerability testing of participating services using anything other than a dedicated test instance provided by ELMO and with ELMO's written consent
- Violating any laws or breaching any agreements in order to discover vulnerabilities.

Such actions are considered a breach of the ELMO Agreement, and may also be considered unlawful activity and subject to criminal prosecution.