Security Policy

Last modified: June 30, 2023

Electrotechnik Pty Ltd (“ELEK”) is committed to providing our software customers with protection against cyber threats, preventing data loss and meeting compliance requirements.

We have adopted the ISO/IEC 27001 principles which is the world’s best-known standard for information security management systems (ISMS). By having this approach in place, we can manage risks related to the security of data owned and handled by our company, whilst ensuring we adopt the best practices and principles for avoiding potential negative impacts due to cyber-crime and new threats that are constantly emerging.

How we provide information security

We are committed to information security to ensure that the stringent systems and controls are in place to maintain information security for our business and customers. We start with our staff onboarding involving processes and company polices which outline the importance of ensuring that all user data remains confidential and that access to such data is only for completing tasks related to their job including providing service to our users. Our Information Security Policy also states the importance of maintaining confidentiality of any user data and the appropriate disposal mechanisms of any locally stored or printed personal data.

Our employees commit to maintaining confidentiality and information security as part of their employment contracts and undertake Cybersecurity Awareness Training, with regular refresher training.

In addition to ELEK’s process, policy, and training, we have strict entry points to access systems containing sensitive user data. Refer to our Privacy Policy for further information.

Identity and access management

We use Microsoft for our enterprise identity provider and highly secure password policies are in use. All employees are required to use 2-factor authentication (2FA) for logging in.

Access to our cloud services in Amazon Web Services (AWS) is granted with AWS Identity and Access Management (IAM) based on role with the need-to-know and least privilege principles.

A quarterly user access review is conducted where access that is no longer necessary is removed. When employees terminate their employment all access to systems is revoked immediately upon exit.

Email protection

We use Microsoft 365 as our staff email provider, Amazon Simple Email Service (SES) for sending emails from within our application and email ticketing system for sending customer support emails. DMARC and SPF are in place for our email domains.

Employees are continuously made aware of and instructed regarding phishing avoidance best practices.

Network security

The workstations of our staff are on a dedicated Virtual Local Area Network (VLAN) that is restricted for use of our staff only.

Access to user data

We treat all data that users submit to any of our software services, which is processed by us solely on a user's behalf, as a "black box". This means that user data is generally not accessed for the performance of the service, and that we handle all submitted user data with the highest level of security and treat it with sensitivity and confidentiality.

Access to user data by our staff is limited in accordance with our Terms of Use or respective agreement with the user, on a case-by-case basis.

Vulnerability management

We regularly perform security audits of our website and software code base to find and fix known vulnerabilities in dependencies that could cause data loss, service outages, unauthorized access to sensitive information, or other security issues. Any vulnerabilities identified are recorded in a development backlog and classified based on our evaluation of their impact on the confidentiality, integrity, and availability of the service and of user data. Our engineers carry out any remediation according to our internal Patch Management Policy.

Software development lifecycle

We use issue tracking products with a well-documented workflow involving a peer review process. Our source code is secured in private, highly secure repositories for version control

and security. Changes to our code base go through a series of automated and manual tests (with detailed plans). Code changes that are approved are first pushed to a staging server where our employees can test changes before an eventual push to production servers and our user base. Our Continuous Integration / Continuous Deployment (CI/CD) process is restricted with an integrated approval process.

Incident response

We take incident management seriously and have an Incident Response Procedure that outlines how incidents are managed. An incident is defined as an unplanned event such as a data breach, interruption to service or a reduction in quality of a service. An incident is also an issue that has been raised where the service previously worked and now does not work as expected. The procedure outlines how we assess, contain, evaluate, notify, review, and monitor incidents.

All incidents are recorded in the Incident Response Register and learnings from incidents are used to improve our process, procedures, systems, and tools as part of our commitment to continuous improvement.

Disaster recovery and Business continuity

We maintain a Business Continuity Plan for dealing with disasters affecting our physical office (where no part of our production infrastructure is retained).

In addition, we maintain a Disaster Recovery Plan (DRP) for dealing with disasters affecting our production environment, that were assessed as critical unplanned events as part of the Incident Response process, which includes the restoration of the service's core functionality from another location. Our primary data centre is hosted on AWS in Sydney (Australia), with redundancy in the same AWS region. In the event of a single AWS data centre loss, recovery procedures would bring up nodes in another data centre without human intervention. Testing is conducted at least once a year. Our DR test may be in the form of a walk-through, mock disaster, or component testing.

Data retention and disposal

Data retention

We retain limited information about you that we solely control for the purpose and the period necessary to fulfill the purposes outlined in our Privacy Policy. Data that our systems hold on behalf of our users will be retained in accordance with our Terms of Use Policy and other commercial agreements with such customers.

We provide both cloud-based and natively installed PC-based software products. With our cloud-based software products the customer data is stored in our secure cloud-based systems (described herein). On the other hand, with our PC-based software products the customer data is stored locally on their IT infrastructure.

Data deletion

Our customers retain full control of their submitted data, and may modify, export, or always delete it either using the means available through our software or through contacting us.

Upon termination of an account, users can request deletion of their data as part of the account closure procedure. User data will then be deleted within 90 days of the request, which includes a 30-day period to allow for rollback and an additional 60 days to proceed with the deletion process.

Alternatively, users may opt to keep the account's data in the platform, in which case we may continue to retain it, but may also delete it at any time at our discretion.

Data destruction

Our cloud services are hosted on AWS who implement secure data distribution and deletion strategies to allow for safe storage of sensitive data in a multi-tenant environment. Storage media decommissioning is performed by AWS according to NIST 800-88.

Monitoring

We collect and monitor network logs using traffic logs from edge locations and load balancers, application-level logging for tracing and auditing events, and system-level logging for auditing access and high-privilege operations. All logs are securely stored in either Amazon S3 or Amazon CloudWatch and are retained.

We monitor the capacity utilization of infrastructure resources to ensure service delivery matches service level agreements. In addition:

- Amazon services are used to trigger automated event-based messaging for critical infrastructure alerts.
- We use proprietary error logging and tracking service with trigger automated event-based messaging for application alerts.

Privacy

Refer to our Privacy Policy.

Office security

Access to our office space, and lifts is restricted via access cards. Building security have several procedures in place to routinely monitor the building and floor access. The security system embedded on each floor tracks door usage, and an access report can be obtained from building security. The desk spaces are under 24-hour CCTV coverage and the premises also have roving security guards across the precinct. CCTV video records are stored and held for 18 months. The Chief Commercial Officer is responsible for updating the Building Management Team of any changes to employees to obtain or revoke access to a building access card.

Data centre security

We rely on the AWS Data Centre controls such as site selection, redundancy, availability, and capacity planning to maintain an appropriate level of security. We do not host any of its own servers.

Policy Updates

This Policy may change from time to time and is available on our website www.elek.com

Contact Us

For further information or to contact us, please visit our contact page.