Version 1.3 Updated 25.05.2022

elastic.io

Elastic.io GmbH
Information Security Management Criteria and Related Controls

Description of Hiring Practices	
Recruiting checks	Multiple interviews and plausibility checking of CVs are documented. Employee onboarding process is recorded in compliance with ISO-27001.
Information security training	Data security awareness trainings and workshop processes are in place for employees and external consultants – executed by our in-house Information Security Management Officer.
Other regulatory compliance training	All employees are informed of their obligations to adhere to GDPR best practices and have signed the 'GDPR Emergency Plan' as part of the employee onboarding process. All employees have undergone information security awareness training. Upon employment all employees are required to sign a Confidentiality Agreement / NDA which extends beyond the direct period of employment.

Incident Response Plan	
Incident Response Plan	Documented as part of ISO-27001. The Incident Management Process is granular in its description of incidents and the responsibilities throughout the management of an incident, including communication channels, both internal and customer-facing.
Communication of incidents	Dependent on Incident level, the Service Level Agreement in place, and our legal responsibilities. We have a list of all contractual and legal requirements on the basis of which we inform our customers in the event of an incident.

Who will communicate the incident?	The communication of an incident to customers will be made by elastic.io management. Internal communication responsibilities are well defined and span all relevant functions.

Business Continuity	
Disaster Recovery Plan	A Disaster recovery plan is in place and is documented as part of ISO-27001. Internal and external communication in the event of a major disruptive incident is defined. Automated processes allow us to rebuild and reconfigure the entire platform in a different cloud infrastructure in the shortest possible time. The disaster recovery process is tested quarterly.
Secondary data center	Hosting on Google Cloud – EU & NA data centers. Identical security policies apply at both.

Information Security	
IT Security Policy	In place – compliant with ISO-27001 and documented. This policy forms the basis of employee and contractor trainings.

<table>
<tr><td>Encryption of data</td><td>Data at rest within the elastic.io platform, such as user data, system credentials, and Kubernetes storage are encrypted using state of the art algorithms.

Data in transit to elastic.io is presented by the respective system e.g. Salesforce according to their standards.

Data in transit within the elastic.io platform are encrypted as standard using state of the art methods.

All internet-facing microservices employed within the elastic.io platform encrypt data as standard.</td></tr>
<tr><td colspan="2"><i><u>Logical Separation</u></i></td></tr>
<tr><td>User access</td><td>Role based access management exists based on PoLP. Customer Admins (contract Owners) are able to assign rights at the level of individual users (3 roles at Contract Level, 5 roles at Workspace Level) and to segregate Users into Teams and define their workspace access.

User authentication via MFA is enabled and users are required to re-authenticate when undertaking sensitive actions such as credential changes or deleting flows.

elastic.io employee and contractor access rights are distributed according to ISO-27001 processes and PoLP. Employee and Contractor access is reviewed and approved by management.

Tenant Admins (client-side) may customise user roles as appropriate for their organisation. Platform structure heirarchy:
Tenant>Contract>Workspace>Flow</td></tr>
<tr><td>Password parameters</td><td>Secure password must be at least 8 characters long and contain at 3 of 4 of the following: upper case (A-Z), lower case (a-z), number (0-9) and special symbols (e.g. ~!@#$%^&*()_+-,.<>?/`|;:'[]=)
OEM customers running their own instance of elastic.io are able to define their own password requirements.</td></tr>
</table>

Password security & reset	Five failed login attempts result in a lock out of the user. These 5 attempts may be a combination of failed login and failed MFA entry, when MFA is enabled. Five failed MFA entries result in user lock out which needs to be resolved by the tenant Admin or elastic.io Support.
Multi-factor Authentication	Yes – configurable by client admins. MFA can be enforced.

Technology Vulnerability Management	
Vulnerability Scans/Assessments & Penetration Testing	
Vulnerability scans	Each code commit is scanned for both dependencies and vulnerabilities. Deploys are automatically blocked when vulnerability or dependency issues are detected.
Vulnerability awareness	Employees are requested to identify vulnerabilities. We are also informed by e-mail from an independent provider about all newly found vulnerabilities within the software products we use.
Penetration tests	Annual Pentest. Scope is the entire elastic.io platform – black-box & grey-box. Testing is subcontracted to an independent professional services organisation.
Response to vulnerabilities	Recorded as part of ISO-27001 processes and treatment agreed according to the Incident Management Plan.
Patch Management	

Identifying and applying patches	Dependencies in our git repositories are identified as part of an automated scanning regime. Dependabot for GitHub is setup for every repository which notifies about vulnerabilities by email immediately after detection. Third-party service providers (e.g. GCP, Docker Hub) send vulnerability notifications.
Patch release	When a vulnerability is detected we confirm its relevance, define its level, and correspondingly create a task and schedule the fix. If level is below 'High' (CVSS <= 8.9), we handle it only if it affects our platform. Each task contains: - CVSS score - from vulnerability description or calculated. - CVE ID if existing - Time-frame for the fix depending on customer affected We send a notification for each affected customer with information contained in the task created. After the fix, we notify customers regarding the corrective actions made.

Backup Frequency/Methods	
Frequency of back-ups	Platform back-ups are performed daily i.e. every 24 hours.
Method of data back-up	Back up DB (Users, flows, workspaces structures). Backup of all our source code repositories. Backup of access information for our platform.
Responsibility for the storage and retention of back-up data	Elastic.io GmbH
Back-up data location	Multiple locations in Google Cloud. In addition, elastic.io source code is updated quarterly and retained by an external service provider.
Back-up data lifetime	Backup is held for 30 days.

Third-Party Service Providers	
Subservice providers	Google Cloud - hosting Freshdesk - ticketing MongoDB – storage Greylog – logging ElasticSearch – Search engine Github – Source Code repository Zenhub – Project Management Clickhouse – Logging data AWS – DNS DPAs are in place with each of the above. Each provider is annually checked regarding their Information Security Management system as part of our supplier audit process.

Physical Security Measures	
Facility access controls at data centers	Not relevant - Google Cloud hosted. GCP DPA exists.