SECURITY QUESTIONNAIRE

CAIQ-Lite v4.1.0.

Generator Labs' answers to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire, Lite edition.

DOCUMENT	CAIQ-Lite v4.1.0 Self-Assessment
SERVICE	Generator Labs (all products)
PUBLISHED	November 2026
CONTACT	legal@generatorlabs.com · generatorlabs.com/security

The Consensus Assessments Initiative Questionnaire (CAIQ) is the Cloud Security Alliance's standard set of security questions for cloud services, mapped to its Cloud Controls Matrix (CCM). This is our self-assessment against the Lite edition: 138 questions across 17 control domains.

Our security program is modeled on ISO 27001 and the SOC 2 Trust Services Criteria. We aren't certified. Each answer below is Yes (implemented), No (not implemented, with the reason and any compensating controls) or N/A (out of scope). Generator Labs owns every control unless a customer responsibility is noted. Our Data Processing Addendum, subprocessor list and security overview are at generatorlabs.com/security, and a summary of our latest penetration test is available on request, with the full report and our policies under NDA, from legal@generatorlabs.com.

133	3	2
YES	NO	NOT APPLICABLE

01

A&A

Audit & Assurance

A&A-02.1 **Are independent audit and assurance assessments conducted according to relevant standards at least annually?** — NO

No SOC 2 or ISO 27001 audit is planned. Our Information Security Program is modeled on the ISO 27001 controls and the SOC 2 Trust Services Criteria, and the Service is penetration tested at least once a year by a third-party service (AWS Security Agent).

A&A-03.1 **Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?** — NO

No formal audit program. The Security Officer reviews the program yearly and after significant changes, and findings from penetration tests go into the risk register.

A&A-04.1 **Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?** — YES

Our Information Security Program lists the laws, regulations, and contracts that apply; compliance with them is reviewed yearly.

A&A-06.1	**Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?** Findings from audits, assessments, and penetration tests go into the risk register with severity, owner, and due date, and are fixed on our patch timelines.	**YES**
A&A-06.2	**Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?** The risk register, including open findings, is reviewed quarterly by the Security Officer.	**YES**

02 Application & Interface Security

AIS

AIS-02.1	**Are baseline requirements to secure applications established, documented, and maintained?** Written coding standards cover secure query handling (parameterized or escaped values only), strict typing, and container hardening. PHP code is checked with PHPStan at level 9.	**YES**
AIS-04.1	**Is a secure SDLC process defined and implemented for application requirements analysis, planning, design, development, testing, deployment, and operation per organizationally designed security requirements?** Changes are developed against written standards, tested on a separate development cluster, and released through a defined process (version, tag, release notes, staged rollout). Static analysis runs on application code.	**YES**
AIS-06.1	**Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?** Every service is built as a container image from a versioned Dockerfile and deployed through versioned task definitions using the same release process.	**YES**
AIS-06.2	**Is the deployment and integration of application code automated where possible?** Image builds, task definition revisions, and rollouts are scripted.	**YES**
AIS-07.1	**Are application security vulnerabilities remediated following defined processes?** Critical security updates are applied within 7 days of release and high-severity updates within 30 days.	**YES**
AIS-07.2	**Is the remediation of application security vulnerabilities automated when possible?** Container images apply all OS package updates at build time on every release. Server patching is scripted.	**YES**

AIS-08.1 **Are processes, procedures, and technical measures defined and implemented to secure APIs?** **YES**

The API requires per-account credentials over TLS 1.2 or 1.3, and every request is scoped to the calling account. Web endpoints have per-client rate limiting.

Customer responsibility: Keep API credentials secret and rotate them if exposed.

AIS-08.2 **Are reviews and updates for any improvements conducted at least annually, or upon significant changes?** **YES**

API and application security practices are reviewed yearly.

03 Business Continuity Management and Operational Resilience

BCR

BCR-01.1 **Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?** **YES**

The Information Security Program (approved, reviewed yearly and after significant changes) includes business continuity and disaster recovery.

BCR-01.2 **Are the policies and procedures reviewed and updated at least annually, or upon significant changes?** **YES**

The Information Security Program (approved, reviewed yearly and after significant changes) includes business continuity and disaster recovery.

BCR-02.1 **Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?** **YES**

Our Information Security Program sets recovery targets from the business impact analysis: recovery point objective of 5 minutes for our database cluster and 24 hours for other data, and recovery time objective of 8 hours for the portal and API. The targets cover the loss of a server, database, or availability zone.

BCR-02.2 **Are the risk assessment and impact analysis reviewed and updated at least annually or upon significant changes?** **YES**

The business impact analysis, targets, and plan are reviewed yearly and after significant changes.

BCR-03.1 **Are strategies being established to reduce the impact of business disruptions, and are resiliency and recovery from business disruptions being improved?** **YES**

Our database cluster spans multiple availability zones and fails over automatically between them. Network egress fails over automatically between availability zones. DNS resolution runs on multiple load-balanced hosts in two Canadian regions.

BCR-08.1 **Are backups performed periodically?** **YES**

Server volumes are backed up daily. Our database cluster has a weekly full backup, daily incremental backups, and continuous transaction log archiving, allowing point-in-time recovery for 30 days.

BCR-08.2 **Is the confidentiality, integrity, and availability of the backup ensured?** **YES**

Backups are encrypted at rest (AES-256) and stored separately from the servers they protect, in versioned object storage with public access blocked, with copies in a second AWS region.

BCR-08.3 **Can backups be restored appropriately for resiliency?** **YES**

A full restore of our database cluster from backup is tested automatically every month and checked for success.

BCR-09.1 **Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?** **YES**

Our Information Security Program documents the recovery plan: the database cluster fails over automatically between availability zones; otherwise, restore the latest backup to a new host, repoint service endpoints, and confirm the restore. Runbooks are kept in the infrastructure record.

BCR-09.2 **Is the disaster response plan updated at least annually, and when significant changes occur?** **YES**

The plan is reviewed yearly and after significant changes.

04 Change Control and Configuration Management

CCC

CCC-01.1 **Are policies and procedures for managing the risks associated with applying changes to assets owned, controlled, or used by the organization established, documented, approved, communicated, applied, evaluated, and maintained?** **YES**

The Information Security Program (approved, reviewed yearly and after significant changes) includes change and configuration management.

CCC-01.2 **Are the policies and procedures reviewed and updated at least annually, or upon significant changes?** **YES**

The Information Security Program (approved, reviewed yearly and after significant changes) includes change and configuration management.

CCC-02.1 **Is a defined quality change control, approval and testing process, incorporating baselines, testing, and release standards, established, maintained and implemented?** **YES**

Changes are tested on a development cluster before release. Releases are versioned and tagged, with release notes, and rolled out service by service.

CCC-04.1	**Is a procedure to authorize the addition, removal, update, and management of assets owned, controlled, or used by the organization, implemented and enforced?** New servers, services, and vendors are added only with Security Officer approval and recorded in the inventory.	YES
CCC-05.1	**Are provisions to limit changes directly impacting service customer-owned environments (tenants) to explicitly authorized requests included within service level agreements?** Customers manage their own configuration in the portal and API. Staff make changes to a customer account only at the customer's request. Customer responsibility: Manage your own account configuration.	N/A
CCC-06.1	**Are change management and configuration baselines established, documented and implemented for all relevant authorized changes on organizational assets?** Servers launch from a maintained, versioned base image. Containers follow a documented baseline: unprivileged user, read-only file system, current OS updates.	YES
CCC-06.2	**Are the baselines reviewed and updated at least annually or upon significant changes?** The base image and container baseline are rebuilt and reviewed as they change, and at least yearly.	YES
CCC-07.1	**Are detection measures implemented with proactive notification if changes deviate from established baselines?** AWS Config records configuration changes and alerts on drift from the baseline.	YES
CCC-09.1	**Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?** Every deployment keeps the previous task definition and function version, so a release can be rolled back to the last known good version.	YES

05 Cryptography, Encryption & Key Management

CEK

CEK-01.1	**Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?** The Information Security Program (approved, reviewed yearly and after significant changes) includes cryptography and key management.	YES

CEK-01.2	**Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually, upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes cryptography and key management.	**YES**
CEK-02.1	**Are cryptography, encryption, and key management roles and responsibilities defined and implemented?** The Security Officer owns cryptography and key management and approves changes to it; administrators operate it.	**YES**
CEK-03.1	**Are data protection at-rest and in-transit, and where applicable in use, provided using cryptographic libraries certified to approved standards?** Encryption at rest uses AWS KMS, whose keys are protected by FIPS 140-validated hardware security modules. TLS is provided by OpenSSL and AWS load balancers.	**YES**
CEK-04.1	**Are encryption algorithms following industry standards utilized for protecting data, based on the data classification and associated risks?** AES-256 at rest, TLS 1.2 or 1.3 in transit, and bcrypt for stored passwords.	**YES**
CEK-05.1	**Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?** Changes to algorithms, protocols, or key handling follow the standard change process and are approved by the Security Officer.	**YES**
CEK-10.1	**Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?** Encryption keys are generated by AWS KMS. Application secrets are generated with the operating system's cryptographic random number generator.	**YES**
CEK-12.1	**Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?** AWS-managed keys rotate automatically. Application secrets are rotated at least yearly, and immediately if exposed or when someone with access leaves. The backup encryption key is replaced if exposed or when someone with access to it leaves.	**YES**
CEK-13.1	**Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?** A compromised key is revoked and replaced at once, and keys are rotated when someone with access leaves.	**YES**

CEK-14.1	**Are processes, procedures and technical measures to securely destroy cryptographic keys when they are no longer needed, defined, implemented, and evaluated, and include provisions for legal and regulatory requirements?** Retired keys are deleted once no data or backup depends on them; AWS KMS handles destruction of AWS-managed keys.	**YES**

06

DCS

Datacenter Security

DCS-04.1	**Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?** The Information Security Program (approved, reviewed yearly and after significant changes) includes workplace and remote work rules. Physical data center security is provided by AWS.	**YES**
DCS-04.2	**Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes workplace and remote work rules.	**YES**
DCS-06.1	**Is the classification and documentation of physical and logical assets based on the organizational business risk?** Data is classified as Confidential, Internal, or Public, and each asset takes the level of the most sensitive data it holds.	**YES**
DCS-06.2	**Are assets' classifications reviewed and updated at least annually or upon significant changes?** The inventory and classifications are reviewed yearly and updated with every change.	**YES**
DCS-07.1	**Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?** Every cloud server, its role, and its data volumes are recorded in a maintained inventory and tagged in AWS. Physical data center assets are managed by AWS.	**YES**
DCS-07.2	**Is the catalogue reviewed and updated at least annually or upon significant changes?** The inventory is updated with every infrastructure change.	**YES**

07

DSP

Data Security and Privacy Lifecycle Management

DSP-01.1	**Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the preparation, classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?** The Information Security Program (approved, reviewed yearly and after significant changes) includes data protection and privacy, alongside the Privacy Policy and DPA.	**YES**
DSP-01.2	**Are data security and privacy policies and procedures reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes data protection and privacy.	**YES**
DSP-03.1	**Is a data inventory created and maintained for sensitive, regulated and personal information (at a minimum)?** Personal data categories, data subjects, and processing locations are documented in Annex 1 of our Data Processing Addendum and in our Privacy Policy.	**YES**
DSP-03.2	**Is the inventory reviewed and updated at least annually or upon significant changes?** Reviewed when the Service or the DPA changes, and at least yearly.	**YES**
DSP-04.1	**Is data classified according to type and sensitivity levels?** Data is classified as Confidential, Internal, or Public, with handling rules for each level.	**YES**
DSP-05.1	**Is data flow documentation created to identify what data is processed and where it is stored and transmitted?** The data inventory (DPA Annex 1) records what personal data is processed and where it is stored and transmitted; subprocessors and their locations are listed publicly.	**YES**
DSP-05.2	**Is data flow documentation reviewed at defined intervals, at least annually, or upon significant changes?** The data inventory and processing locations are reviewed yearly.	**YES**
DSP-06.1	**Is the ownership and stewardship of all relevant personal and sensitive data documented?** Under our DPA the customer is the controller and Generator Labs the processor. Customer responsibility: Act as controller for personal data you submit.	**YES**
DSP-06.2	**Is data ownership and stewardship documentation reviewed at least annually?** Reviewed with the DPA, at least yearly.	**YES**

DSP-07.1	**Are systems, products, and business practices based on security principles by design and per industry best practices?** Databases and internal services run in private networks; containers run unprivileged with read-only file systems; each service has its own least-privilege cloud and database role.	**YES**
DSP-08.1	**Are systems, products, and business practices based on privacy principles by design and according to industry best practices?** The Service collects only what monitoring requires, does not need sensitive data, and does not sell or share personal data.	**YES**
DSP-08.2	**Are systems' privacy settings configured by default and according to all applicable laws and regulations?** Accounts and their data are private by default, and the Service collects only what monitoring needs. Check result pages linked from alerts are reachable only through a random, unguessable 64-character link and are not listed anywhere; customers can turn these links off.	**YES**
DSP-10.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?** All transfers use TLS. International transfers are covered by the EU Standard Contractual Clauses and UK and Swiss equivalents in our DPA.	**YES**
DSP-11.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?** Most requests can be handled by customers in the portal and API. Other requests go to legal@generatorlabs.com and are answered within 30 days. Customer responsibility: Respond to data subject requests about data you control.	**YES**
DSP-12.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?** Customer personal data is processed only on the customer's documented instructions (DPA Section 3).	**YES**
DSP-13.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?** Subprocessors are bound by written data protection terms no less protective in substance than our DPA and listed publicly.	**YES**

DSP-14.1 **Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?** **YES**

Customers get at least 30 days' notice before a new subprocessor processes their data, with a right to object.

DSP-16.1 **Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?** **YES**

Customer data is deleted within 30 days of account closure; backups expire within a further 30 days. Billing records are kept six years as Canadian tax law requires.

DSP-17.1 **Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?** **YES**

Encryption in transit and at rest, role-based access, MFA for administrative access, and deletion on account closure.

DSP-19.1 **Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?** **YES**

Processing and backup locations are documented in our DPA: AWS in the United States (N. Virginia, Ohio) and Canada (Montreal, Calgary). Checks also query third-party sources (such as blocklist operators' DNS servers) and customer-configured endpoints, wherever they're located; these aren't subprocessors.

08 Governance, Risk and Compliance

GRC

GRC-01.1 **Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?** **YES**

The Information Security Program (approved, reviewed yearly and after significant changes) is sponsored and approved by company leadership.

GRC-01.2 **Are the policies and procedures reviewed and updated at least annually, or upon significant changes?** **YES**

The Information Security Program (approved, reviewed yearly and after significant changes) is reviewed at least yearly by the Security Officer.

GRC-02.1 **Is there an established and maintained formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of risks?** **YES**

Our Information Security Program defines risk management: yearly risk assessment, a risk register with owner, likelihood, impact, treatment, and due date, written risk acceptance by the Security Officer, and quarterly review.

GRC-06.1	**Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?** Our Information Security Program defines the roles: the Security Officer owns the program, administrators hold privileged access, and all staff follow it.	**YES**
GRC-07.1	**Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?** Applicable requirements are identified in our DPA and Privacy Policy: GDPR, UK GDPR, Swiss FADP, PIPEDA, CCPA, and Canadian tax record-keeping.	**YES**
GRC-07.2	**Are the identified requirements reviewed at least annually or upon significant changes?** The list of applicable laws and contracts is reviewed yearly.	**YES**

09 Human Resources

HRS

HRS-03.1	**Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?** Staff lock screens when away and keep confidential data out of sight.	**YES**
HRS-03.2	**Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes these rules.	**YES**
HRS-04.1	**Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?** Remote work rules: no confidential data on public or shared devices, trusted networks or a VPN only, and device requirements.	**YES**
HRS-04.2	**Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes these rules.	**YES**
HRS-11.1	**Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?** All staff complete security and privacy awareness training when they join and every quarter after. Completion is recorded.	**YES**

HRS-11.2	**Are regular security awareness training updates provided?** Training is repeated and updated every quarter.	YES

10

IAM

Identity & Access Management

IAM-01.1	**Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?** The Information Security Program (approved, reviewed yearly and after significant changes) includes identity and access management.	YES
IAM-01.2	**Are identity and access management policies and procedures reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes identity and access management.	YES
IAM-03.1	**Is the inventory of identities managed, stored, and regularly reviewed, and is their level of access monitored?** Administrative identities are inventoried and their access is reviewed every quarter.	YES
IAM-04.1	**Is the separation of duties principle employed when implementing information system access?** With a small team, one administrator may build and deploy a change. Compensating controls: every change is versioned and logged, and CloudTrail records all cloud administrative actions.	NO
IAM-05.1	**Is the least privilege principle employed when implementing information system access?** Each service runs with its own cloud role and database role limited to what it needs; no application role has superuser rights. The cloud root account has no access keys. Customer responsibility: Assign portal roles to your users on a least-privilege basis.	YES
IAM-06.1	**Is an identity access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?** Access is requested and approved by the Security Officer and recorded in the access register with the date and approver.	YES
IAM-07.1	**Is a process in place to de-provision or modify identity access in a timely manner?** Access is removed the same day a person leaves or changes role. Customer responsibility: Remove departed users from your account.	YES

IAM-08.1	**Are reviews and revalidation of identity access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance, and at least annually or upon significant changes?** Administrative access is reviewed every quarter.	**YES**
IAM-09.1	**Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated?** Privileged cloud access is separate from service roles, requires MFA, and the root account is not used for daily work.	**YES**
IAM-10.1	**Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?** Administrative access to our cloud infrastructure and database cluster is granted through time-limited sessions: an MFA-assumed role with 1-hour sessions, and on-demand database sessions. Third-party admin consoles are reviewed quarterly.	**YES**
IAM-10.2	**Are procedures implemented to prevent the accumulation of segregated privileged access?** All administrative access is reviewed quarterly, and access is removed the same day a person leaves or changes role.	**YES**
IAM-13.1	**Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?** MFA is required for all administrative access to our cloud infrastructure. Portal users can enable MFA. Account owners can require it for every user and choose how their users sign in, including through supported third-party sign-in providers. Customer responsibility: Enable MFA for your users.	**YES**
IAM-13.2	**Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?** Services authenticate with short-lived cloud role credentials rather than stored keys. Public endpoints use CA-issued TLS certificates.	**YES**

11 Interoperability & Portability

IPY

IPY-01.1	**Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application interfaces (e.g., APIs)?** The Information Security Program (approved, reviewed yearly and after significant changes) includes data portability.	**YES**

IPY-01.2	**Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?** The Information Security Program (approved, reviewed yearly and after significant changes) includes data portability.	**YES**
IPY-01.3	**Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?** The Information Security Program (approved, reviewed yearly and after significant changes) includes data portability.	**YES**
IPY-01.4	**Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?** Customers can export their data through the portal and the documented API, in standard formats.	**YES**
IPY-01.5	**Are interoperability and portability policies and procedures reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes data portability.	**YES**

12

I&S

Infrastructure Security

I&S-03.1	**Are communications between environments, services, and applications monitored?** Amazon GuardDuty monitors network and DNS activity in our cloud environments for threats.	**YES**
I&S-03.2	**Are communications between environments, services, and applications encrypted?** Traffic to the website, portal, and API, and connections that carry customer data inside private networks (load balancer to containers), use TLS 1.2 or 1.3.	**YES**
I&S-03.3	**Are communications between environments, services, and applications restricted to only authenticated and authorized connections, as justified by the business?** Security groups and network ACLs limit connections to what each service needs, and databases and caches require authentication.	**YES**
I&S-03.4	**Are network configurations reviewed at least annually?** Network configuration is reviewed yearly.	**YES**

I&S-03.5	**Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?** Every allowed security group and network ACL rule has a documented purpose in the infrastructure record.	**YES**
I&S-04.1	**Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?** Servers launch from a minimal, maintained base image with IMDSv2 required; containers run unprivileged with read-only file systems; AWS hardens the hypervisor and control plane.	**YES**
I&S-06.1	**Are applications and infrastructures designed, developed, deployed, and configured such that service customer (tenant) access is appropriately segmented, segregated, monitored, and restricted?** Every customer request is scoped to the customer's own account in code, and each account has its own credentials.	**YES**
I&S-07.1	**Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?** All migrations and administrative transfers use TLS or encrypted AWS management channels.	**YES**
I&S-09.1	**Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?** AWS Shield Standard DDoS protection, AWS WAF on the public load balancer, security groups and network ACLs, per-client rate limiting, Amazon GuardDuty threat detection, and alarms on error rates and availability that alert on-call staff.	**YES**

13

LOG

Logging and Monitoring

LOG-01.1	**Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?** The Information Security Program (approved, reviewed yearly and after significant changes) includes logging and monitoring.	**YES**
LOG-01.2	**Are policies and procedures reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes logging and monitoring.	**YES**

LOG-04.1	**Is audit log access restricted to authorized identities, and are records of that access maintained?** Audit log access is restricted to administrators, and every read of the audit logs is itself logged (CloudTrail data events on the audit log bucket).	**YES**
LOG-05.1	**Are capabilities implemented and maintained to correlate and monitor security audit logs for the detection of suspicious or anomalous activity that deviates from typical or expected patterns?** Amazon GuardDuty continuously analyzes cloud audit, network, and DNS activity for suspicious or anomalous behaviour and alerts on-call staff.	**YES**
LOG-05.2	**Is a process established and followed to review and take appropriate and timely actions on detected anomalies?** Alarms page on-call staff, who investigate and act on them.	**YES**
LOG-08.1	**Are technical measures defined, implemented, and evaluated to enable service customers to detect and scrub or tokenize sensitive data from logs, in order to prevent unauthorized exposure as per applicable laws and regulations?** Customers have no access to our system logs.	**N/A**

14

SEF

Security Incident Management, E-Discovery, & Cloud Forensics

SEF-03.1	**Is a security incident response plan that includes a communication strategy for notifying relevant internal departments, impacted service customers, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?** Our incident response plan covers severity levels, response steps, and notification of affected customers within 72 hours and of regulators as the law requires.	**YES**
SEF-04.1	**Is a structured approach followed to evaluate the effectiveness of incident response plans at planned intervals or upon significant changes?** The incident response plan is tested at least yearly with a tabletop exercise and updated with what we learn.	**YES**
SEF-07.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated for timely and effective response to security incidents in accordance with incident categories and severity levels?** Affected customers are notified within 72 hours, regulators as the law requires, with updates as more is known.	**YES**

SEF-07.2	**Are these processes and procedures reviewed, updated, and tested at least annually?** The plan, including notification, is reviewed and tested yearly.	**YES**
SEF-08.1	**Are processes, procedures, and technical measures for security breach notifications defined and implemented?** We notify affected customers within 72 hours of becoming aware of a security incident affecting their data (DPA Section 7).	**YES**
SEF-08.2	**Are material security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?** As committed in our DPA and required by applicable law.	**YES**

15

STA

Supply Chain Management, Transparency, and Accountability

STA-01.1	**Are policies and procedures for supply chain risk management established, documented, approved, communicated, applied, evaluated, and maintained?** The Information Security Program (approved, reviewed yearly and after significant changes) includes vendor management.	**YES**
STA-01.2	**Are policies and procedures for supply chain risk management reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes vendor management.	**YES**
STA-03.1	**Is the SSRM applied, documented, implemented, and managed throughout the supply chain?** Responsibilities shared with vendors (for example AWS for physical security and the hypervisor) are recorded in this questionnaire and reviewed yearly with each vendor.	**YES**
STA-05.1	**Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM?** Ownership for each control is given in this questionnaire.	**YES**
STA-08.1	**Is an inventory of all supply chain relationships developed and maintained?** Subprocessors are listed publicly; other vendors are tracked internally.	**YES**

16

TVM

Threat & Vulnerability Management

TVM-02.1	**Are policies and procedures to protect against malware and malicious instructions established, documented, approved, communicated, applied, evaluated, and maintained?** The Information Security Program (approved, reviewed yearly and after significant changes) includes malware protection and device anti-malware.	**YES**
TVM-02.2	**Are asset management and malware protection policies and procedures reviewed and updated at least annually, or upon significant changes?** The Information Security Program (approved, reviewed yearly and after significant changes) includes malware protection.	**YES**
TVM-03.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?** Container images are scanned on every build and weekly (Trivy). Amazon Inspector scans EC2 instances and Lambda functions continuously in every region we use. Findings are tracked in the risk register.	**YES**
TVM-05.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?** Amazon GuardDuty threat intelligence and detection models are updated continuously by AWS.	**YES**
TVM-08.1	**Are processes, procedures and technical measures defined, implemented and evaluated based on identified risks to support scheduled and emergency responses to vulnerability identification?** Scheduled patching on fixed windows; emergency patches are applied out of cycle, for example same-day redeployment of all services for a critical kernel CVE.	**YES**
TVM-10.1	**Is a risk-based method used for the prioritization and mitigation of threats, leveraging an industry-recognized framework to guide threat decision-making and protection measures?** Vulnerabilities are prioritized by vendor severity rating or CVSS, with fix deadlines of 7 days (critical), 30 days (high), and 90 days (medium), and low severity in the next scheduled patch cycle.	**YES**
TVM-11.1	**Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?** Every finding is recorded in the risk register with severity, owner, and due date, closed when verified fixed, and reviewed quarterly.	**YES**

17

UEM

Universal Endpoint Management

UEM-02.1	**Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?** Staff devices install software only from the operating system's official store or the vendor's official site.	**YES**
UEM-04.1	**Is an inventory of all endpoints used and maintained to store, access and process company data?** Every staff device that accesses company data is recorded in the device register.	**YES**
UEM-05.1	**Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?** Device requirements are set in our Information Security Program, and compliance is checked every quarter with a signed checklist for each device, recorded in the device register. A failing device loses access until fixed.	**YES**
UEM-06.1	**Are all relevant interactive-use endpoints configured to require an automatic lock screen?** Devices lock automatically after 10 minutes of inactivity; checked quarterly.	**YES**
UEM-09.1	**Are anti-malware detection and prevention technology services configured on managed endpoints?** Anti-malware is required and turned on on every device; checked quarterly.	**YES**
UEM-10.1	**Are software firewalls configured on managed endpoints?** The operating system firewall is required and turned on on every device; checked quarterly.	**YES**
UEM-13.1	**Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?** Every device can be wiped remotely, or has its company access revoked at once if lost; checked quarterly.	**YES**



Questions About Our Security?

Our Data Processing Addendum, subprocessors and security overview are on our security page. For our penetration test summary, policies or anything this questionnaire doesn't answer, email legal@generatorlabs.com.

generatorlabs.com/security

© 2026 GENERATOR LABS · ALL RIGHTS RESERVED · GENERATORLABS.COM