Security, Privacy, Architecture and Compliance

Lightico Corporate Trust commitment

Lightico is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our services, including protection of Customer Data.

Services Covered

This document describes the architecture of, the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to the Lightico SaaS platform.

General Company Policies

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand Lightico's objectives. The assigned policy owner updates the policy annually and the policy is reviewed and approved by designated members of management. In addition, Responsibility and accountability for developing and maintaining the policies are assigned to the relevant Lightico teams and are reviewed and approved on an annual basis by the management team. Policies and procedures are documented, reviewed and approved on an annual basis by the management team and available to Lightico's employees within Lightico's internal portal.

Security and Architecture

Lightico provides a secure, reliable and resilient Software-as-a-Service platform that has been designed from the ground up based on industry best practices. The following addresses the network and hardware infrastructure, software and information security elements that Lightico delivers as part of this platform, database management system security, application controls and intrusion detection monitoring software.

Data Center Security

Lightico relies on Amazon Web Services global infrastructure, including the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of basic computing resources and storage. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards: FedRAMP, HIPAA, ISO 27001:2015, AICPA SOC 1, SOC 2, SOC 3 and PCI-DSS and more. The environmental protection managed by the vendor's policies are:

- Redundancy - The data centers are designed to anticipate and tolerate failure while maintaining service levels with core applications deployed to multiple regions.
- Fire Detection and Suppression – Automatic fire detection and suppression equipment has been installed to reduce risk.
- Redundant Power – The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure. Data centers use generators to provide back-up power for the entire facility.
- Climate and Temperature Controls – Maintain a constant operating temperature and humidity level for all hardware.
- Physical access - AWS recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas.

Infrastructure Security

End-to-End Network Isolation - the Virtual Private Cloud is designed to be logically separated from other cloud customers and to prevent data within the cloud being intercepted.

- External & Internal enforcement points - All servers are protected by restricted AWS firewall rules. The configuration of AWS firewall rules is restricted to authorized personnel.
- Server Hardening - all servers are hardened according to industry best practices.
- Segregation Between Office and Production Networks – there is a complete separation between the Lightico Corporate network and the Production network. Access to the production environment is granted to authorized personnel only, and traffic between the networks is sent over an encrypted tunnel.

Application Security

- **Penetration Testing** - A penetration test is performed on a semi-annual basis. High issues are investigated and taken care of as part of the SDLC process or by any necessary means. The penetration tests include, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. In addition, security scans are performed on a semi-annual basis. The penetration tests and security scans are performed by a reputable third-party vendor.
- **Vulnerabilities Management** - Web application architecture and implementation follow OWASP guidelines. The application is regularly tested for common vulnerabilities (such as CSRF, XSS, SQL Injection). Vulnerability scans are performed to the production environment on a quarterly basis, using an external tool, in order to detect potential security breaches.
- **Segregation of Customer Data** - Lightico employs a login system and authorization mechanism based on industry best practices. During each user request, a validation process is performed through encrypted identifiers to ensure that only authorized users gain access to the specific data. The process is validated by third-party security consultants on a yearly basis.
- **Web Application Firewall (WAF)** - Lightico implemented a world class WAF to prevent application security issues and DDOS attacks.
- **Static Code analysis and Code reviews** - Lightico is committed to secure coding process as part of Lightico’s SDLC policy. Static Code analysis is performed on an ongoing basis.

Operational Security

Configuration and Patch Management – Lightico employs a centrally managed configuration management system, including infrastructure-as-code systems through which predefined configurations are enforced on its servers, as well as the desired patch levels of the various software components.

Security Incident Response Management - Whenever a security incident of a physical or electronic nature is suspected or confirmed, Lightico’s engineers are instructed to follow appropriate procedures. Security Incident Response Policy is documented, reviewed and approved on an annual basis by the management team and available to Lightico employees. Customers and legal authorities will be notified as required by Privacy regulations.

Antivirus - An antivirus/malware solution is installed on employees’ laptops in order to detect and prevent infection by unauthorized or malicious software. Antivirus reports are sent to relevant stakeholders on a regular basis. Anti-virus definition updates are performed and monitored on a regular basis by the Security team. The employees’ laptops are encrypted with the use of a 256-bit AES encryption.

End point Detection and Response (EDR) - Lightico’s EDR is focused on providing the right endpoint visibility with the right insights to help security analysts discover, investigate and respond to very advanced threats and broader attack campaigns stretching across multiple endpoints.

Data Encryption

Data on Transit - All traffic between the customers and the Lightico platform is encrypted, only TLS 1.2 or higher versions are enabled. In addition, Lightico uses an HTTPs protocol internally between the servers.

Data at Rest – Lightico files at rest are encrypted using 256-bit Advanced Encryption Standard (AES).

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to one or more of the Covered Services, as described below.

ISO 27001/27701 certification: Lightico operates an information security management system (ISMS) for the Covered Services in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. The Lightico ISO 27001/27701 Certificate and Statement of Applicability are available upon request.

Service Organization Control (SOC) reports: Lightico's information security control environment applicable to the Covered Services undergoes an independent evaluation in the form of SOC 2 audits Lightico's most recent SOC 2 reports are available upon request.

Payment Card Industry (PCI): For the Covered Services, Lightico has obtained an Attestation of Compliance ("AOC") demonstrating SP Level 1 compliance with the applicable Payment Card Industry (PCI) Data Security Standard (DSS). A copy of Lightico's AOC is available upon request.

HIPAA: To support all Lightico businesses that are in the healthcare and wellness industries, we have redesigned our privacy rules to make sure that we are in compliance with the requirements of the HIPAA Privacy Rules.

GDPR: As an organization focused on trust and careful handling of customer data, Lightico has been committed to privacy since inception. Our strong compliance culture and robust security safeguards, which are reflected in our ISO 27001 and Soc 2 type 2 Compliance, provide a solid foundation for ongoing GDPR compliance efforts.

Availability Procedures

Lightico's production environment is fully managed as part of the AWS services and monitored by Lightico's Operations team using the tools provided by AWS as well as additional internal tools. The application level is fully managed by the Lightico Security team. Admin access to the Lightico platform is restricted to authorized personnel. Lightico has implemented the operations management controls described below to manage and execute production operations.

Database Backup

Lightico's databases are hosted at AWS. The Lightico application database is backed up daily as according to the backup policy. The snapshots are replicated every day and fully on a weekly and monthly basis. The backup system automatically generates a backup log. In case of failure, a notification is sent to the Operations team. The access to the backup and offline storage is restricted to authorized individuals. The company holds a replica of each data center for high-availability standards in case of a disaster.

Restoration

A restore process is performed and documented on an annual basis (minimum). The backup data captured as part of the daily, weekly and monthly backup procedures is restored automatically into a separate environment in order to determine the integrity of the data and potential data recovery issues. A log of the restoring process is sent to the DevOps team for review.

Data center availability procedures

AWS provides Lightico with a secured location implementing security measures to protect against environmental risks or disaster. Lightico databases are replicated to 3 different availability zones. Lightico maintains a backup server infrastructure at a separate location within the AWS environment.

Business Continuity Plan (BCP)

Lightico has developed a Business Continuity Plan to enable the company to continue to provide critical services in the event of a disaster. Lightico maintains a backup infrastructure at a separate location within the AWS environments. The backup server's infrastructure has been designed to provide clients with business-critical services until the disaster will be contained and the primary system is fully restored. The alternative processing environment is wholly managed by appropriate Lightico personnel, as is the case with the primary production environment.

Monitoring Usage

The management team receive updates on an annual basis on availability, security, confidentiality and privacy non-compliance issues that may come up and address them as needed. Such issues are documented as part of a support process and if necessary, notifications are sent to the Security team or the IT and Information Security Officer. Change reports, vulnerability reports from production and monitoring tools as well as support metrics are reviewed and discussed in relation to the organization's security system, availability, confidentiality and privacy policies. In addition, environmental, regulatory and technological changes are monitored. Their effects are assessed, and their policies are updated accordingly. A summarized protocol is made available to relevant managers and team members.

Disaster Recovery Plan (DRP)

Lightico has developed a Disaster Recovery Plan in order to continue to provide critical services in the event of disaster. The DRP is tested on an annual basis. Lightico maintains a backup plan and configuration for each critical service within the AWS environments. The backup plan and configuration has been designed to provide clients with business-critical services until the disaster effects have been resolved and the primary system is fully restored. The alternate processing environment is wholly managed by appropriate Lightico personnel, as is the case with the primary production environment.

Privacy Procedures

The Lightico Privacy statement is available on the company website and fully discloses the type of information Lightico may collect from the Lightico application, as well as how Lightico may use this information. Contact information is available on the company web page, providing mailing addresses, phone numbers, and email addresses for submitting privacy inquiries and complaints.

Lightico retains personal information in accordance with the company's Privacy Policy.

The Lightico privacy policy is reviewed and updated by management on an annual basis.

Lightico's privacy commitments are communicated to employees via an Information Security Policy document detailing the secure handling of company confidential information, including customer data.

Lightico's privacy commitments and updates are communicated to customers via email.

Lightico disposes of personal information in accordance with the company's Privacy Policy.

Lightico obtains privacy commitments through contracts with third parties who have access to their personal information. Email communications from third parties are used in the event of a suspected unauthorized disclosure of personal information.

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the Covered Services is retained in inactive status within the Covered Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Lightico uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, Lightico reserves the right to reduce the number of days it retains such data after contract termination. Lightico will update this Lightico Security, Privacy, Architecture and Compliance Documentation in the event of such a change.

About Lightico

Lightico's platform for digital customer interactions empowers businesses to collect forms, documents, e-signatures, photos, payments, consent to disclosures and to verify ID instantly, even while they have customers on the phone.