TECHNICAL AND ORGANIZATIONAL MEASURES FOR LASTPASS

Security and Privacy Operational Controls

Publication date: February 2022

1 Products and Services

This document describes the Technical and Organizational Measures (TOMs) for LastPass. LastPass is a password management and single sign-on (SSO) solution that enables users to securely store, create and access their user identity and login credentials for online applications and websites.

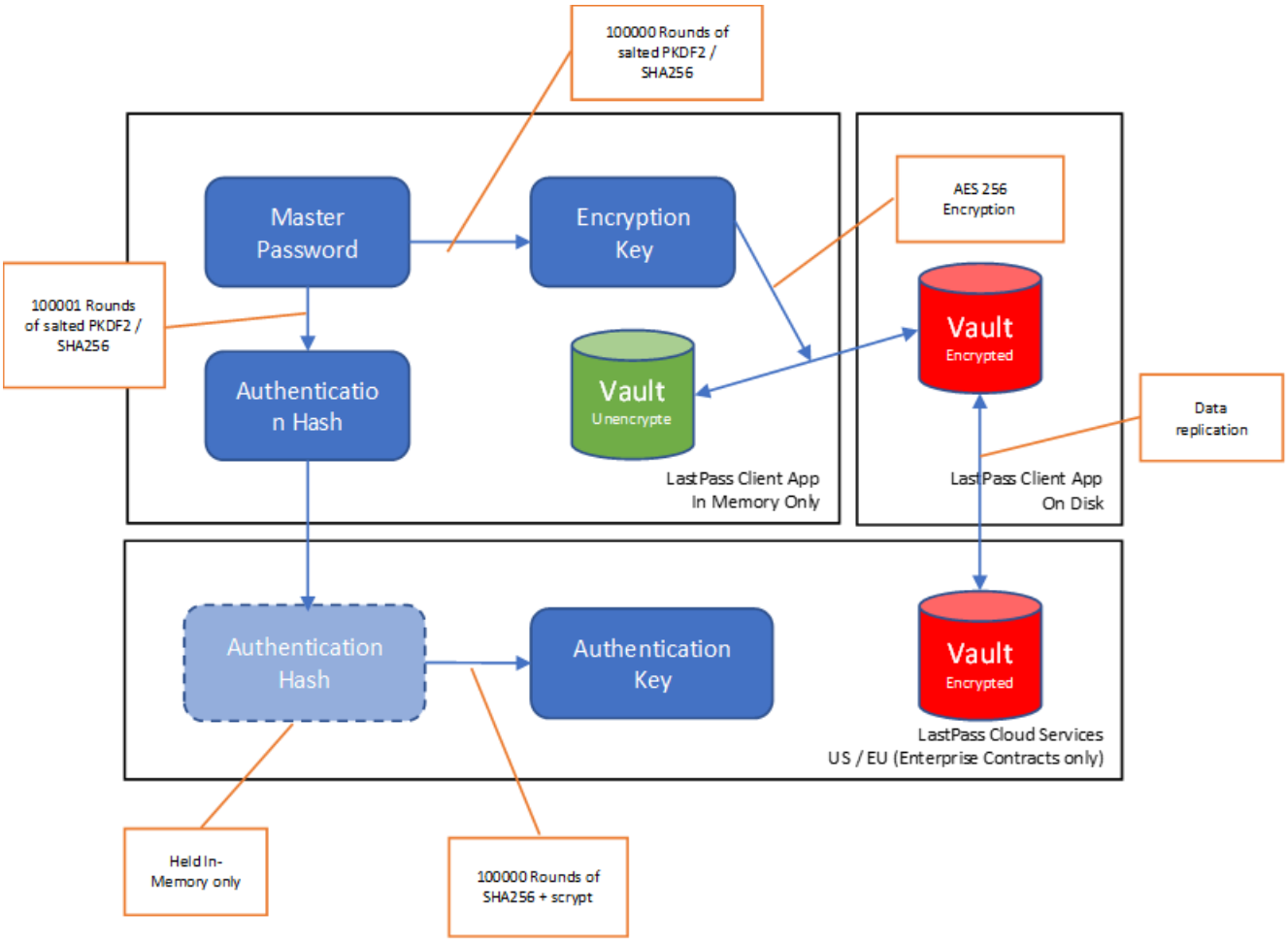
LastPass Enterprise: LastPass Enterprise now includes single sign-on (SSO) technology, with a robust catalog of 1,200+ pre-integrated apps, in addition to its existing market leading password management capabilities. LastPass Enterprise manages access for every entry point in a single solution.

LastPass Multi-Factor Authentication (MFA): Going beyond standard two-factor authentication (2FA), LastPass MFA is designed to ensure that only the right users are accessing the right data at the right time, without unnecessary added complexity. Through the use of biometric factors like face and fingerprint ID coupled with contextual factors such as geolocation and IP address, LastPass MFA offers an intuitive authentication experience that's seamless for employees to use and easy for admins to deploy across cloud, legacy, on-premise apps and VPN.

LastPass Identity: LastPass Identity combines the features of LastPass Enterprise and LastPass MFA and provides a holistic view of end-user activity from a single dashboard that covers passwords, authentication, and all apps in use.

2 Product Architecture

The LastPass service features a vault, in which sensitive user data is stored and, based on utilization of a 'zero-knowledge' framework, accessed only by entering the user's master password, which is not maintained in unencrypted form by LastPass -- LastPass does not store and cannot access this password. User data input via the LastPass web or mobile application is encrypted with the user's unique key on their device and the AES-256 encrypted data is synced to LastPass for secure storage. The user can access and decrypt their data on demand with their master password – which occurs entirely at the user and device-level.



The LastPass infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using, depending on data residency preferences (i.e., elected during account creation): (a) redundant, active-passive datacenters in the United States or Europe; or (b) world-class cloud hosting provider data centers in Australia, Singapore, India or Canada. All datacenters are located in hosted cloud or co-location facilities that monitor environmental conditions and provide around-the-clock physical security.

Further, LastPass offers offline access, which means that a user without an internet connection can still access a version of its encrypted vault (cached on their device from their last login) through the LastPass browser extension or mobile application. For details about the LastPass architecture, please refer to the LastPass Technical Whitepaper.

3 LastPass Technical Controls

LastPass employs industry standard technical security controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service) designed to safeguard the Service infrastructure and data residing therein. Find the Terms of Service at https://www.goto.com/company/legal/terms-and-conditions.

3.1. Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in both the corporate and production environment. Employees are granted minimum (or “least privilege”) access to specified LastPass systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

3.2. Perimeter Defense and Intrusion Detection

LastPass employs industry standard perimeter protection tools, techniques, and services that are designed to prevent unauthorized network traffic from entering our product infrastructure. These include, but are not limited to:

- Intrusion detection systems that monitor systems, services, networks, and applications for unauthorized access
- Critical system and configuration file monitoring to prevent or reduce the likelihood of unauthorized modification
- A hosted and/or cloud-based application firewall and application-layer DDoS prevention service through which LastPass traffic is proxied, designed to block malicious server traffic
- A local application firewall that provides an additional layer of protection against OWASP top ten and other web application vulnerabilities and malicious traffic
- Host-based firewalls on LastPass web servers that filter inbound and outbound connections, including internal connections between LastPass systems

3.3. Data Segregation

LastPass leverages a multi-tenant architecture, logically separated at the database level, based on a user’s or organization’s LastPass account. Only authenticated parties are granted access to relevant accounts.

3.4. Physical Security

LastPass contracts with datacenters to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant datacenter
- Scheduled maintenance and validation of all critical security and environmental controls

LastPass limits physical access to production data centers to authorized individuals only. Access to an on-premise server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations. LastPass management reviews physical access logs to data centers and server rooms on at least a quarterly basis. Additionally, physical access to data centers is removed upon termination of previously authorized personnel.

3.5. Data Backup, Disaster Recovery and Availability

LastPass operates, based on data residency preference (elected at new account creation), in: (a) fully redundant, active-passive datacenters in the United States or Europe; or (b) world-class cloud hosting provider data centers in Australia or Singapore. LastPass Password Manager and LastPass SSO functionalities are separated in distinct data centers. Each datacenter is capable of handling all LastPass user traffic.

All user data is stored in a redundant manner with automatic disaster recovery and failover using multiple datacenters.

LastPass backs-up Customer Content within the same datacenter in 24-hour and seven-day intervals. In addition, a corresponding back-up is made in a geographically distant datacenter every seven days and is retained for four weeks.

To ensure the safety of your data the LastPass SSO database leverages 7-day point-in-time restore (PITR) capability. Additionally, Long-Term Retention (LTR) backup will keep the first backup of a week for four weeks and the first backup of each month for three months as an additional safety feature.

If enabled, a secure, encrypted, local copy of a user's vault is stored automatically when a user connects to LastPass via a browser extension or mobile application. This cached version is designed to allow the user offline access to their data and vault when no internet connection is available.

3.6. Malware Protection

Malware protection software with audit logging is deployed on all LastPass servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

3.7. Encryption

LastPass maintains a cryptographic standard that aligns with recommendations from industry trade groups, government publications, and other relevant standards groups. This standard is periodically reviewed and, if deemed appropriate, selected technologies and ciphers may be updated.

LastPass utilizes cryptography to defend against brute-force password attacks. Sensitive data stored within a user's LastPass vault is encrypted using a unique encryption key that LastPass does not possess. This key is derived from a user's master password.

User Authentication

To authenticate a user against the LastPass server, LastPass generates an authentication token by hashing a user's master password and email, now with a default 100,000 rounds of PBKDF2 with SHA-256 client-side, before sending the token to the server. The server then performs another 100,000 rounds of SHA-256 and script before comparing the result to a value stored in LastPass' database to determine if authentication was successful.

Vault Encryption at Rest

The LastPass browser extension or mobile application utilizes PBKDF2 with SHA-256 to derive a unique encryption key from a user's master password. This encryption key remains on the user's device (and is never received by LastPass) and is used to encrypt vault data with the AES-256 algorithm. On Windows devices, Windows Crypto APIs are used to add an extra layer of protection. The encrypted vault is transmitted over TLS to LastPass, and stored server-side in this encrypted state. In addition, the locally encrypted vault is cached on the user's device (after login), enabling offline access if needed.

SSO Encryption at Rest

LastPass SSO uses transparent data encryption, that encrypts the storage of the entire database by using a symmetric key called the database encryption key. This database encryption key is protected by the transparent data encryption protector, – a service-managed certificate.

On database startup, the encrypted database encryption key is decrypted and then used for decryption and re-encryption of the database files in the SQL Server Database Engine process. Transparent data encryption performs real-time I/O encryption and decryption of the data at the page level. Each page is decrypted when it's read into memory and then encrypted before being written to disk.

The built-in server certificate is unique for each server and the encryption algorithm used is AES 256. As the databases are in a geo-replication relationship, both the primary and geo-secondary database are protected by the primary database's parent server key. LastPass SSO temporarily stores SAML certificates for processing on encrypted storage using 256-bit AES encryption.

The certificates are automatically rotated in compliance with the internal security policy and the root key is protected by an internal secret store.

Encryption in Transit

To safeguard Customer Content in transit, it is first encrypted using AES-256 CBC mode and then again via Transport Layer Security (TLS) protocols when sent over HTTPS. In addition, LastPass uses the latest version of Secure Shell (SSH) with strong cipher suites for specified administrative functions.

In general, connectivity to sensitive systems and services including access to LastPass internal networks is protected by appropriate transport encryption technologies.

3.8. LastPass Enterprise Functionality

Master Password Reset

LastPass Enterprise offers “Super Admin” functionality, in which the enterprise can assign select administrators (deemed Super Admins) master password reset rights that provide them the ability to reset a user’s master password.

If Super Admins are assigned, when a new user is created or a master password is changed, a copy of the user's local key, used to encrypt and decrypt their vault, is encrypted to the Super Admin account. Only the Super Admin account can decrypt the local key to initiate a master password reset. LastPass does not allow Super Admins to access the contents of a user's vault via this functionality – only master password resets are permitted.

3.9. Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to the relevant development teams, as well as management.

3.10. Logging and Alerting

LastPass collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

LastPass maintains a comprehensive set of organizational and administrative controls designed to protect the security and privacy posture of LastPass.

4.1. Security Policies and Procedures

LastPass maintains a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2. Standards Compliance

LastPass complies with applicable legal, financial, data privacy, and regulatory requirements, and maintains compliance with the following certifications and external audit reports:

- TRUSTe Enterprise Privacy & Data Governance Practices Certification to address operational privacy and data protection controls that are aligned with key privacy laws and recognized privacy frameworks. To learn more, please visit our blog post.

- American Institute of Certified Public Accountants' (AICPA) Service Organization Control (SOC) 2 Type 2 attestation report. BSI Cloud Computing Catalogue (C5).
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- Payment Card Industry Data Security Standard (PCI DSS) compliance for LastPass's eCommerce and payment environments
- Internal controls assessment as required under a Public Company Accounting Oversight Board (PCAOB) annual financial statements audit

4.3. Security Operations and Incident Management

LastPass's Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with LastPass's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve relevant suspected or identified security events across its systems and Services, including LastPass. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the LastPass intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4. Application Security

LastPass's application security program follows the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis, and system hardening. In addition, LastPass participates in a bug bounty program (https://bugcrowd.com/lastpass) hosted by BugCrowd, which encourages external security researchers to responsibly disclose potential security vulnerabilities.

4.5. Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6. Security Awareness and Training Programs

New hires are informed of security policies and the GoTo Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team. LastPass employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire

onboarding kits, awareness campaigns, webinars with the CISO, a security champion program and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices

LastPass takes the privacy of its Customers, subscribers to the LastPass Services, and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1. GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. LastPass is compliant with the applicable provisions of GDPR. For more information, please visit https://www.goto.com/company/trust/privacy.

5.2. CCPA

LastPass hereby represents and warrants that it is in compliance with the California Consumer Privacy Act (CCPA). For more information, please visit https://www.goto.com/company/trust/privacy.

5.3. Data Protection and Privacy Policy

GoTo is pleased to offer a comprehensive, global Data Processing Addendum (DPA), available in English and German, to meet the requirements of the GDPR, CCPA, and beyond and which governs LastPass's processing of Personal Data.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including: (a) data processing details, sub-processor disclosures, etc. as required under Article 28; (b) EU Standard Contractual Clauses (also known as the EU Model Clauses); and (c) inclusion of LastPass's technical and organizational measures. Additionally, to account for CCPA coming into force, we have updated our global DPA to include: (a) revised definitions which are mapped to CCPA; (b) access and deletion rights; and (c) warranties that LastPass will not sell our users' 'personal information.'

For visitors to our webpages, GoTo discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on the public website. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.4. Transfer Frameworks

LastPass has a robust global data protection program which takes into account applicable law and supports lawful international transfers under the following frameworks:

5.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (or “SCCs”) are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the European Economic Area (“EEA”) will be transferred in compliance with EU data-protection law. LastPass has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. LastPass offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope LastPass services as part of its global DPA. Execution of the SCCs helps ensure that LastPass customers can freely move data from the EEA to the rest of the world.

Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created the following FAQ designed to outline its supplemental measures utilized to support lawful transfers under Chapter 5 of the GDPR and address and guide any “case-by-case” analyses recommended by the European Court of Justice in conjunction with the SCCs.

5.4.2 APEC CBPR and PRP Certifications

GoTo has additionally obtained Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") and Privacy Recognition for Processors ("PRP") certifications. The APEC CBPR and PRP frameworks are the first data regulation frameworks approved for the transfer of personal data across APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance.

5.5. Return and Deletion of Customer Content

LastPass users can delete their own accounts and associated Content via the “Delete your Account” page located at https://lastpass.com/delete_account.php. Users without access to their LastPass vault and/or email address can submit a service request to the Care team, who will authenticate the user and delete the account and Content within 30 days of the request.

Free accounts, including the Content located therein, shall automatically be deleted after two (2) years of inactivity (i.e., no logins).

5.6. Sensitive Data

While LastPass aims to protect and safeguard all Customer Content, regulatory and contractual limitations require us to restrict the use of LastPass for certain types of information. Unless Customer has written permission from LastPass, the following data must not be uploaded or generated to LastPass:

- Government-issued identification numbers and images of identification documents.
- Information related to an individual’s health, including, but not limited to, Personal Health Information (PHI) as identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as other relevant applicable laws and regulations.

- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7. Tracking and Analytics

LastPass is continuously improving its websites and products using third-party web analytics tools which help LastPass understand how visitors use its websites, desktop tools, and mobile applications, as well as user preferences and problems. For further details please reference the Privacy Policy.

6 Third Parties

6.1. Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates third-party hosting facilities and vendors that provide information security-based services. Legal and Procurement may evaluate relevant contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes. Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or are granted access to sensitive or confidential data by LastPass are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2. Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, LastPass reviews relevant third party's terms and conditions and either utilizes LastPass-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting LastPass

Customers can contact LastPass at https://support.goto.com for general inquiries or privacy@goto.com for privacy-related questions.