LastPass

LastPass Technical and Organizational Measures (TOMs)

Security and Privacy Controls

Last updated January 2025

1 Products and Services

LastPass is an award-winning password manager and provider of password and identity management solutions (“Services”) for individuals, families, teams and businesses. The LastPass Password Manager employs a zero-knowledge security model and robust encryption to safeguard passwords and sensitive data, as well as to enable the secure sharing of credentials and other items within customer vaults.

LastPass enhances online security and privacy by helping customers create unique and complex passwords to facilitate secure access to resources across most popular devices, operating systems, and web browsers, featuring a user-friendly interface, automatic form filling and other features such as dark web monitoring and an online identity security score to help measure security hygiene.

For businesses, LastPass also provides features such as centralized user management, a rich policy engine to govern use of the Services, federated integration with identity providers, native integrations with popular security event and information management (“SEIM”) tools, and a multi-factor authentication application for mobile platforms, addressing enterprise-level security and compliance requirements.

LastPass has implemented and will maintain the following technical and organizational measures which have been designed for the protection, availability, authenticity, integrity, and confidentiality of Personal Data submitted to LastPass by or on behalf of customers in connection with their use of the Services.

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.

LastPass utilizes a globally distributed infrastructure designed to increase service reliability and reduce the risk of downtime from single points of failure LastPass operates, depending on data residency preferences (i.e., as specifically elected by customer during account creation), redundant, active-passive cloud regions in the United States, Europe, Australia, Singapore, India, or Canada.

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 additional details about the LastPass product architecture, please refer to the LastPass Technical Whitepaper.

3 LastPass Technical Controls

LastPass employs 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. You can find the LastPass Terms of Service at https://www.lastpass.com/legal-center/terms-of-service.

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 environments. 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.

We protect our systems by implementing multi-factor authentication and conditional access policies to decrease opportunities for misuse.

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 and botnet activities; and
- Endpoint Detection and Response agents on LastPass web servers that protect 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 world-class cloud hosting providers to maintain physical security and environmental controls for server rooms that house production servers. These controls typically 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, and
- Scheduled maintenance and validation of all critical security and environmental controls.

Our hosting providers limit, control, and manage physical access to their infrastructure through robust practices aligned and audited yearly against the highest security standards.

3.5 Data Backup, Disaster Recovery, and Availability

LastPass utilizes a globally distributed infrastructure designed to increase service reliability and reduce the risk of downtime from single points of failure. LastPass' most up-to-date list of regional providers and their geographic location may be found within the Sub-processors Disclosure at the LastPass Trust and Privacy Center (also accessible via https://www.lastpass.com/trust-center/resources).

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

LastPass backs-up Customer Content within our geographically distant regions in 24-hour and seven-day intervals and is retained for 18 months.

To ensure the safety of your data the LastPass SSO database leverages 35-day point-in-time restore (PITR) capability. Additionally, we retain two-hour backups for seven days and weekly backups that we retain for 18 months as an additional safety feature.

If enabled, a secure, encrypted, copy of a user's vault is also automatically stored locally 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 vault data, even when no internet connection is available.

3.6 Malware Protection

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

3.7 Cryptography

LastPass implements cryptographic mechanisms, certificate management controls, and other controls for the confidentiality, integrity, and authentication of data at rest and data in transit. These cryptographic mechanisms and processes align with industry standard practices and regulatory requirements. LastPass maintains a Cryptography Policy that sets clear requirements for cryptography, and routinely evaluates those requirements while taking into account the state of the art and industry changes.

LastPass utilizes cryptography throughout its Services to protect the confidentiality of users and their vault data and for user authentication.

Encryption in Transit

LastPass uses transport layer security (TLS) that incorporates perfect forward secrecy cipher suites for the protection of data in transit.

3.8 Vulnerability Management

LastPass has established a Vulnerability Management Program (VMP) to ensure comprehensive oversight and governance of people, processes, and technologies, with the aim of identifying and remediating vulnerabilities that impact LastPass IT assets and infrastructure in a risk-based manner, while ensuring compliance with industry standards and best practices for vulnerability management.

LastPass leverages industry-leading vulnerability scanning tools to regularly scan its IT assets, infrastructure, and code repositories. This includes scanning employee laptops to identify vulnerabilities in the software used by staff, as well as assessing its cloud infrastructure and resources to detect vulnerabilities, misconfigurations, and opportunities to enhance overall security posture.

Additionally, LastPass scans software developed and maintained internally by scanning code in repositories and during the build process, using Static Application Security Testing (SAST) tools, along with manual code reviews by the Application Security team. These practices are integral to the software assurance process, ensuring the security and integrity of the code that supports LastPass products and services. Additionally, LastPass conducts regular external vulnerability scans of its internet-exposed environments, utilizing traditional vulnerability scanning methods and Dynamic Application Security Testing (DAST) to identify vulnerabilities that could potentially impact production environments. In addition, LastPass conducts scheduled penetration testing exercises on a recurring basis throughout the year to further assess and identify vulnerabilities that may not have been detected by automated scanning tools.

3.9 Logging and Alerting

We collect logs and alerts from our platform components and security controls in our XDR (Extended Detection) and response / SOAR (Security Orchestration, Automation and Response) system which are received, triaged, assessed and responded to by one or more of our Security Operations, Threat intelligence, and other internal stakeholders depending on scope and severity.

3.10 LastPass Admin Functionality

The LastPass service provides configurable security features which enable customers and their admins to drive good security hygiene and minimize poor security practices that may put their data at risk. Customers can manage directory integration, user management, security policies, and advanced security features from their admin console.

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 and Privacy Policies and Procedures

LastPass maintains a comprehensive set of security and privacy 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. More information is available at the LastPass Trust and Privacy Center at https://www.lastpass.com/trust-center.

4.2 Third-Party Security Audits

LastPass is committed to continually assessing and enhancing the security of its organization and safeguarding customer data through comprehensive evaluation processes, including third-party audits and security testing. As part of this commitment, LastPass commits that its products and services undergo annual security assessments and attestations conducted by multiple reputable, independent third-party security vendors. More information is available at the LastPass Trust and Privacy Center at https://www.lastpass.com/trust-center.

4.3 Security Operations and Incident Management and Response

LastPass has implemented and maintains a Security Incident Response Plan (SIRP), Information Security Incident Management Policy, and associated standard operating procedures, which are aligned with the National Institute of Standards and Technology (NIST) Cyber Incident Handling guide and applicable regulatory requirements. These policies and procedures are designed to help LastPass respond to and manage relevant suspected or identified security events that may impact LastPass employee or customer data and systems and, depending on the nature of the incident and relevant requirements, facilitate notification to our customers within applicable timeframes.

4.4 Application Security

LastPass's application security program follows industry best practices to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, software composition analysis, container and infrastructure as code scanning, 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. 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

Mandatory annual security and privacy training is provided to personnel appropriate to their job function. 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 and security team, and other methods and practices. New hires are informed of security policies and the LastPass Code of Conduct and Business Ethics at orientation.

4.7 Return and Deletion of Customer Content

LastPass has implemented policies and procedures designed to ensure that Personal Data will not be retained and used unless necessary to provide Services or as outlined in our agreements with you. LastPass provides customers with the ability to manage its users and retrieve or delete Customer Content via detailed instructions located at https://support.lastpass.com/.

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 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, are automatically deleted after two (2) years of inactivity (i.e., no logins or activity associated with the account).

4.8 Cross Border Data Transfers

LastPass has a robust global data protection program which takes into account applicable law and supports lawful international transfers and utilizes, as applicable and required, lawful data transfer mechanisms. LastPass applies safeguards, in accordance with applicable legal requirements, so that the data recipient provides an adequate level of data protection.

4.8.1 Data Privacy Framework

LastPass complies with the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF") as set forth by the U.S. Department of Commerce. LastPass has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles ("EU-U.S. DPF Principles") and the Swiss-U.S. Data Privacy Framework Principles ("Swiss-U.S. DPF Principles") with regard to the processing of personal data received from the European Union, United Kingdom, and Switzerland.

4.8.2 Standard Contractual Clauses

Standard Contractual Clauses (or “SCCs”) are standardized contractual terms, recognized and adopted by regulators. 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.

4.8.3 CBPR and PRP Certifications

LastPass obtained 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 member countries and were obtained and independently validated through TrustArc, an approved third-party leader in data protection compliance.

5 Third Parties

5.1 Use of Third Parties

As part of supply chain risk management, LastPass conducts appropriate due diligence on third party service providers depending upon relevancy and applicability. The evaluation includes a review of third party’s technical and organizational measures that maintain the confidentiality, integrity, and availability of the Services and data. Depending on the nature of the third-party’s services, other appropriate compliance documentation or reports may be obtained and evaluated to verify the control environment is functioning adequately and any necessary user consideration controls are addressed.

5.2 Contract Practices

Third parties that host or have access to confidential or sensitive data are required to enter into a written agreement outlining relevant requirements regarding, when applicable business continuity and measures are in place to protect the confidentiality and integrity of 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.

6 Contacting LastPass

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