TECHNICAL AND ORGANIZATIONAL MEASURES FOR LASTPASS SECURITY AND PRIVACY OPERATIONAL CONTROLS
Technical and Organizational Measures for LogMeIn LastPass
Security and Privacy Operational Controls

Publication Date: September 2021

1. Products and Services
This document describes the security and privacy controls 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 or Singapore. 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 Security Controls
LogMeIn 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 www.logmein.com/legal/terms-and-conditions.
4 Organizational Controls
LogMeIn 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
LogMeIn 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
LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and conform with the following compliance certifications and external audit reports:

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. 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 LogMeIn’s eCommerce and payment environments
- Internal controls assessment as required under a Public Company Accounting Oversight Board (PCAOB) annual financial statements audit
- 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.

4.3 Security Operations and Incident Management
LogMeIn’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 LogMeIn’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 LogMeIn intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.
4.4 Application Security
LogMeIn’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 LogMeIn Code of Conduct and Business Ethics at orientation. Further, mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

LogMeIn employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire on-boarding kits, awareness campaigns, webinars with the CISO, a security champion program, and the display of posters and other collateral in major corporate offices, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices
LogMeIn takes the privacy of its Customers, the subscribers to the LogMeIn 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. Central/Pro is compliant with the applicable provisions of GDPR. For more information, please visit http://www.logmeininc.com/trust/privacy.

5.2 CCPA
LogMeIn hereby represents and warrants that it is in compliance with the California Consumer Privacy Act (CCPA). For more information, please visit www.logmeininc.com/trust/privacy.
5.3 Data Protection and Privacy Policy
LogMeIn 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 LogMeIn’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 LogMeIn'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 LogMeIn will not sell our users’ ‘personal information.’

For visitors to our webpages, LogMeIn 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
LogMeIn 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. LogMeIn has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. LogMeIn offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope LogMeIn services as part of its global DPA. Execution of the SCCs helps ensure that LogMeIn customers can freely move data from the EEA to the rest of the world.

Supplemental Measures
In addition to the measures specified in this SPOC, LogMeIn 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
LogMeIn 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 LogMeIn 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 LogMeIn, 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) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations
- Any information especially protected by applicable laws and regulation, specifically information about an individual’s race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7 Tracking and Analytics
LogMeIn is continuously improving its websites and products using various third-party web analytic tools, which help LogMeIn understand how visitors use its websites, desktop tools, and mobile applications; what they like and dislike; and where they may have 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 LogMeIn 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, LogMeIn reviews relevant third party’s terms and conditions and either utilizes LogMeIn-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting LogMeIn
Customers can contact LastPass support at https://support.logmeininc.com/ for general inquiries or privacy@logmein.com for privacy-related questions.