LAMBDATEST

Technical & Organizational Measures

Version Number: 1.2

Table of Contents

1. Overview

Our top priorities are confidentiality, security, integrity, privacy, and availability of customer information. We know how vital it is to your business's success. To ensure you never have to worry, we use a multi-layered approach to protect and monitor all your information. LambdaTest has implemented multiple technical and organizational measures.

2. Information Security Program

2.1. LambdaTest maintains a written information security program that:

i. is managed by a senior employee responsible for overseeing and implementing the program.

ii. includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, availability, and privacy of Customer Data as required by Data Protection Law(s) and best practices

iii. is appropriate to the nature, size, and complexity of LambdaTest's business operations.

iv. agrees to regularly test, assess, and evaluate its program's effectiveness to ensure processing security.

2.2. LambdaTest follows the ISO 27001 control standard framework cross-reference with NIST SP 800-53 Rev 5, SOC 2, CSA, PCI DSS, HIPAA, GDPR, CCPA, etc.

2.3. LambdaTest has comprehensive privacy and security assessments and certifications performed by third parties. Such certifications include SOC 2 Type II, ISO 27001, 27017, and 27701 standard certifications.

3. Product Development and Platform Security

3.1. Security by Design: LambdaTest has adopted security by design principles throughout the product development lifecycle and this helps us to manage information security, cybersecurity, data security, and privacy consideration or related risk by default and by design.

3.2. LambdaTest leverages a modern and secure open-source framework and other third-party libraries with security controls to limit exposure to OWASP Top 10 security risks.

3.3. Vulnerability Management and Platform Security Assessment: LambdaTest runs the internal and external system and network vulnerability scans at least quarterly and after any major system and network configuration change. LambdaTest also utilizes a qualified third party to conduct the platform security assessment at least annually.

3.4. LambdaTest evaluates and tracks vulnerabilities of open source software (OSS) and other 3rd party libraries that are incorporated into the LambdaTest platforms. LambdaTest performs static code analysis and manual code review, as required by the risk management process. Security verification, including penetration testing and multiple dynamic analysis tools, are conducted by third-party firms and security researchers.

3.5. Change Management: LambdaTest uses the Scrum model from the agile framework in combination with the Continuous Integration and Continuous Deployment (CI/CD) approach to ensure faster delivery of functionalities to its customers. Also, LambdaTest employs a documented change management program with respect to the products as an integral part of its security profile. This includes logically or physically separating environments from production for all development, testing, and staging.

3.6. Version Control: Source code is managed centrally with version controls and restricted access based on various teams assigned to specific sprints. Records are maintained for code changes and code check-ins and check-outs.

4. Application Access Control and Security

4.1. LambdaTest adopts and follows **"**least privilege**,"** **"**need-to-know**,"** and **"**need-to-have or need-to-do-principles**"** **provisions** for access rights. These are applied across all information systems, applications, and services.

4.2. LambdaTest access control mechanisms can detect, log, and report access to the system and platform or application or attempt to breach security of the system or platform.

4.3. LambdaTest supports Single Sign-On (SSO) through SAML 2.0.

4.4. Segregation of Duties: Access to the production environment is limited to a set of employees based on the job roles as they need this access for any configuration or troubleshooting. These privileges access are reviewed regularly.

4.5. LambdaTest configures remote access to all systems and networks, and the production environment is allowed only from the LambdaTest corporate networks that are behind VPN. All the access is protected via Single Sign On (SSO) or multi-factor authentication, and all accesses will be logged.

4.6. Password hashing: User account passwords stored on LambdaTest Service are bcrypt hashing with a random salt using industry-standard techniques.

4.7. LambdaTest development team is trained on Open Web Application Security Project (OWASP) secure coding practices and uses industry-best practices for building secure platforms or applications. The application security team conducts whitebox testing on each code release and blackbox testing on third-party software to mitigate risk.

4.8. LambdaTest production environment is logically segregated from the development, testing, and staging environment with concepts of virtual private cloud and subnets. No customer data and test execution data are used in our development or test environments.

4.9. LambdaTest trains its employees to treat data protection and security as the highest priorities. LambdaTest is committed to implementing tighter security standards across policies, procedures, technology, and people on an ongoing basis.

4.10. Multi-Tenancy: Each application is serviced from an individual virtual private cloud, and each customer is uniquely identified by a tenant ID. The application is engineered and verified to ensure that it always fetches data only for the logged-in-tenant. Per this design, no customer has access to another customer's data.

5. Infrastructure and Network Security

5.1. Architecture: LambdaTest network security architecture consists of multiple security zones. More restricted systems like database servers are protected in our most trusted zones. Other systems are hosted in zones commensurate with their sensitivity, depending on function, information classification, and risk. Depending on the zone, additional security monitoring and access controls will apply. DMZs are utilized between the internet and internally between the different zones or trusts.

5.2. LambdaTest Security Incident Event Management (SIEM) system gathers extensive logs from important network devices and host systems. The SIEM alerts on triggers that notify the security team based on correlated events for investigation and response.

5.3. Intrusion Detection and Prevention: Service ingress and egress points are instrumented and monitored to detect abnormal behavior. These systems are configured to generate alerts when incidents and values exceed predetermined thresholds and use regularly updated signatures based on new threats. This includes 24/7 system monitoring.

5.4. DDoS Mitigation: LambdaTest has architected a multi-layer approach to DDoS mitigation. A core technology partnership with Cloudflare provides network edge defenses, while the use of AWS scaling and protection tools provide deeper protection along with our use of AWS DDoS-specific services.

5.5. LambdaTest deploys firewall technology in the operation of LambdaTest's production environment. Traffic between Customer and LambdaTest will be protected and authenticated by industry-standard cryptographic technologies.

5.6. LambdaTest regularly updates network architecture schemas and maintains an understanding of the data flows between its systems. Firewall rules and access restrictions are reviewed for appropriateness regularly.

5.7. Applications and servers are regularly patched to provide ongoing protection from exploits.

6. Storage, Handling and Disposal

6.1. Data Segregation- LambdaTest logically separates and segregates Customer Data from its other Customer's data.

6.2. Encryption of Data- LambdaTest utilizes industry-standard encryption algorithms and key strength to encrypt all Customer Data while in transit over all networks (e.g., Internet). Data at rest is encrypted using AES-256 bit standards with keys being managed by key management services, and data in transit is encrypted using HTTPs with TLS 1.2 and above over a secure socket connection for accounts hosted in the LambdaTest domain (LambdaTest.com).

6.3. Destruction of Data- Customer data is disposed of in a method that renders the data unrecoverable, to the extent reasonably possible, in accordance with industry best practices for wiping of electronic media (e.g., NIST SP 800-88).

7. Business Continuity and Disaster Recovery

7.1. LambdaTest has a formal Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) defined and implemented to enable people, process, and technology support during any crisis or business interruptions. Appropriate roles and responsibilities have been defined and documented. LambdaTest Customer Success team will be responsible for communication and notification during a crisis.

7.2. The BCP and DR Plan is tested and reviewed on a yearly basis by the LambdaTest Information Security Officer (ISO) and approved by ISCSC (Information Security & Compliance Steering Committee). On a yearly basis, training on BCP and DRP requirements is provided to all relevant workforce members involved in the process.

The BCP and DR plan of LambdaTest is reviewed and audited as part of ISO 27001 standards and SOC 2 Type II covering availability as one of the trust service principles.

7.3. LambdaTest's Disaster Recovery Plan includes, but is not limited to, infrastructures, technology, and system(s) details, recovery activities, and identifies the people/teams required for such recovery, exercised at least annually.

7.4. Availability & Continuity: LambdaTest maintains a publicly available platform-heath dashboard, which includes platform, or system availability details, scheduled maintenance, service incident history, and relevant security events.

7.5. Redundancy: LambdaTest employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime and/or our DR service offering allow us to deliver a high service availability, as account or Test execution data is replicated across availability zones.

7.6. LambdaTest Disaster Recovery services add contractual objectives for Recovery Time Objective (RTO) and Recovery Point Objective (RPO). These are supported through our capability to prioritize operations of DR during any declared disaster events.

- 4-hour Recovery Time Objective (RTO): LambdaTest will aim to restore normal operations for the LambdaTest platform account within four hours from the time a disaster is declared, unless a disaster, or multiple disasters, impacts all the Availability Zones used on an account.
- Under 1-hour Recovery Point Objective (RPO): LambdaTest will target one hour or less of data loss of customer accounts. This is calculated from the point of the disruption, not from LambdaTest's disaster declaration.

8. Due Diligence over Sub-Processors/Contractors

LambdaTest partners with organizations that, like itself, adhere to global standards and regulations. These organizations include sub-processors or third parties that LambdaTest utilizes to assist in providing its services. The list of sub-processors, along with their roles in processing and their processing location, are disclosed in the following link: https://www.lambdatest.com/legal/sub-processor

8.1. Maintain a security and privacy process to conduct appropriate due diligence prior to engaging sub-processors or third-party vendors.

8.2. Assess the security and privacy capabilities of any such sub-processors or vendors to adhere to LambdaTest policies.

8.3. Apply written information security and compliance requirements that oblige sub-processors or vendors to adhere to LambdaTest key information security and privacy policies and standards consistent with and no less protective than these measures.

8.4. Regular assessments are conducted on such sub-processors or vendors to ensure data is processed in a fair manner, and that data is processed only for the purposes it was collected. Apart from evaluation for technical requirements, an examination for data protection measures, compliance with LambdaTest's security and privacy requirements, and audit reports review is conducted before on-boarding the sub-processors or vendors.

8.5. Various checks on the sub-processors or vendors' vulnerability and patch management processes for intrusion protection capabilities are reviewed. Copies of the access management process, third-party vulnerability testing reports, SOC 2 reports, ISO 27001 /27701 reports, PCI DSS AOC, etc. are shared by the service partner and reviewed by LambdaTest.

9. Security Incident and Breach Notification

9.1. Security Incident: LambdaTest has defined the security incident management process to classify and handle incidents and security breaches. The information security team is responsible for recording, reporting, tracking, responding, resolving, monitoring, reporting, and promptly communicating about the incidents to appropriate parties. The process is reviewed as part of periodic internal audit and is audited as part of ISO 27001 and SOC 2 Type II assessment.

9.2. Notice of Personal Data Breach:

- LambdaTest as data controller- we notify the concerned Data Protection Authority of the breach within 72 hours after we become aware of it. Depending on specific requirements, we will notify Customers too, when necessary.
- LambdaTest as data processors- we will notify the concerned data controllers (customers) promptly and without undue delay of actual or potential personal data breaches or exposure of customer data relating to a personal data breach as it becomes known or as is reasonably requested by the customer.
- LambdaTest's notification of a Personal Data Breach will describe, to the extent possible, the nature of the Personal Data Breach, the measures taken to mitigate the potential risks, and the measures that LambdaTest recommends the customer take to address the Personal Data Breach.
- The Data Protection Officer is responsible for reporting to customers about personal data breaches.

You may contact our 24x7 hotline at privacy@lambdatest.com or security@lambdatest.com to report complaints/breaches.