675 Massachusetts Avenue, 10th Floor
Cambridge, MA 02139-3309

(866) 787 7030

hello@litmus.com

Information Security at Litmus

Updated 1 March 2018 | security@litmus.com

Public

Table of Contents

1. Purpose, Scope, and Organization

This document defines behavioral, process, technical, and governance controls pertaining to security at Litmus that all personnel are required to implement in order to ensure the confidentiality, integrity, and availability of all Litmus services and data (“Policy”).

This Policy defines security requirements for:

- All Litmus employees, contractors, consultants, and any other third parties providing services to Litmus (“personnel”),
- Management of systems, both hardware and software and regardless of locale, used to create, maintain, store, access, process or transmit information on behalf of Litmus, including all systems owned by Litmus, connected to any network controlled by Litmus, or used in service of Litmus’s business, including systems owned third party service providers, and
- Circumstances in which Litmus has a legal, contractual, or fiduciary duty to protect data or resources in its custody.

In the event of a conflict, the more restrictive measures apply. All personnel must review and be familiar with the rules and actions set forth below.

1.1. Information Security Governance at Litmus

This Policy was created in close collaboration with and approved by Litmus senior executives. This Policy is reviewed annually and modified as needed to ensure clarity, sufficiency of scope, concern for customer and Litmus interests, and general responsiveness to the evolving security landscape and industry best practices. Litmus aligns its Information Security program with ISO 27001 and 27002 security best practices and guidelines.

Executive Point of contact:
Matt Gore
VP of Engineering
mgore@litmus.com

Security point of contact:
Naomi Buckwalter
Director of Information Security
naomi@litmus.com

1.2. Information Security Team

The Litmus information security team oversees the implementation of this Policy, including

- Procurement, provisioning, maintenance, retirement, and reclamation of corporate computing resources,
- All aspects of service development and operation related to security, privacy, access, reliability, and survivability,
- Ongoing risk assessment, vulnerability management, incident response, and
- Security-related human resources controls and personnel training.

1.3. Risk Management Framework

The security team maintains a Risk Management Framework derived from NIST SP 800-39 - “Managing Information Security Risk: Organization, Mission, and System View” and NIST SP 800-30 - “Guide for Conducting Risk Assessments”. Risk assessment exercises inform prioritization for ongoing improvements to Litmus’s security posture, which may include changes to this Policy itself.

Our Risk Management Framework incorporates the following:

- Identification of relevant, potential threats.
- A scheme for assessing the strength of implemented controls.
- A scheme for assessing current risks and evaluating their severity.
- A scheme for responding to risks.

2. Expectations of Litmus Personnel

Litmus is committed to protecting its customers, personnel, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly in the context of its established employment culture of openness, trust, maturity, and integrity.

This section outlines expected personnel behaviors affecting security and the acceptable use of computer systems at Litmus. These rules are in place to protect our personnel and Litmus itself, in that inappropriate use may expose customers and partners to risks including malware, viruses, compromise of networked systems and services, and legal issues.

2.1. Informed Behavior of Litmus Personnel

The first line of defense in information security is the informed behavior of personnel, who play a significant role in ensuring the security of all data. Such behaviors include those listed in this section as well as any additional requirements specified in the employee handbook, specific security processes, and other applicable employee codes of conduct.

Security Awareness Education
All employees and contractors must participate in the Litmus security awareness education program, offered multiple times throughout the year, to inform all users of the requirements of this Policy.

Unrecognized Persons and Visitors
It is the responsibility of all personnel to take positive action to maintain physical security wherever they happen to be working. Personnel must challenge any unrecognized person present in a restricted office location. All visitors to Litmus offices must be signed in and registered as such or accompanied by a Litmus employee.

Clean Desk Policy
Personnel must maintain workspaces clear of sensitive or confidential material and take care to clear workspaces of such material at the end of each workday.

Unattended Devices
Unattended devices must be locked. All devices must have an automatic screen lock function set to automatically activate upon no more than fifteen minutes of inactivity.

Acceptable Use Policy
Systems are to be used for business purposes in serving the interests of the company, and of our clients and partners in the course of normal business operations. Personnel are responsible for exercising good judgment regarding the reasonableness of personal use of systems. Only Litmus-managed hardware and software is permitted to be connected to or installed on corporate equipment or networks and used to access Litmus data. Litmus-managed hardware and software

includes those either owned by Litmus or owned by Litmus personnel but enrolled in the Litmus device management system. All personnel must read and understand the list of prohibited activities outlined in this Policy.

Local Storage Policy

Personnel may not configure work devices to make backups of device data. Instead, personnel are expected to operate primarily “in the cloud” and treat local storage on computing devices as ephemeral. Making a practice of keeping important work artifacts replicated into company-approved secure cloud storage (e.g. Google Docs) ensures that even in the event of a corporate device being lost, stolen, or damaged, such work artifacts are immediately recoverable on a replacement device.

Prohibited Activities

The following activities are prohibited. Under certain conditions and with the explicit written consent of the security team, personnel may be exempted from certain of these restrictions during the course of their legitimate job responsibilities (e.g. planned penetration testing, systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The list below is by no means exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

- Under no circumstances are personnel of Litmus authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Litmus-owned resources.
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Litmus. Violating or attempting to violate the terms of use or license agreement of any software product used by Litmus is strictly prohibited.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Litmus or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology may result in a violation of international or regional export control laws. The appropriate management must be consulted prior to export of any material that is in question.
- Revealing your account password to others or allowing use of your account by others. This includes colleagues, as well as family and other household members when work is being done at home.
- Making fraudulent offers of products, items, or services originating from any Litmus account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties and then only to the extent the warranties are consistent with Litmus’s authorized warranties.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to

access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious or unlawful purposes.

- Except by or under the direct supervision of the security team, port scanning or security scanning, or other such software designed to exploit or find computer, software, or network vulnerabilities.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account or attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Attempting to interfere with or deny service to any other user.
- Providing information about, or lists of, Litmus personnel to parties outside Litmus.
- Installation of software which installs or includes any form of malware, spyware, or adware as defined by the security team.
- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempts to subvert technologies used to effect system configuration of company-managed devices (e.g. MDM) or personal devices voluntarily used for company purposes (e.g. mobile Work Profiles).

2.2. Personnel Systems Configuration, Ownership, and Privacy

Centralized System Configuration

Personnel devices and their software configuration may be managed remotely by Litmus via configuration-enforcement technology. Such technology may be used for purposes including auditing/installing/removing software applications or system services, managing network configuration, enforcing password policy, encrypting disks, copying data files to/from employee devices, and any other allowed interaction to ensure that employee devices comply with this Policy.

Retention of Ownership

All software programs, data, and documentation generated or provided by personnel while providing services to Litmus or for the benefit of Litmus are the property of Litmus unless otherwise covered by a contractual agreement.

Personnel Privacy

While Litmus's network administration desires to provide a reasonable level of privacy, users remain aware that the data they create on the corporate systems remains the property of Litmus. Due to the need to protect Litmus's network, management does not intend to guarantee the privacy of personnel's personal information stored on any network device belonging to Litmus. Personnel are

responsible for exercising good judgment regarding the reasonableness of personal use such as general web browsing or personal email.

Personnel must structure all electronic communication with recognition of the fact that the content can be monitored and that any electronic communication can be forwarded, intercepted, printed, or stored by others.

Litmus reserves the right, at its discretion, to review personnel files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as corporate policies.

2.3. Human Resources Practices

Background Checks
Background checks are conducted on all employees prior to their start date. The consequences of problematic background check results may range from a limitation of security privileges, to revocation of employment offer, to termination.

Security Awareness Education Training
The security team maintains a company-wide security awareness program delivered to all personnel throughout the year. The program covers security awareness, policies, processes, and training to ensure that personnel are sufficiently informed to meet their obligations. Those most responsible for maintaining security at Litmus, including the security team itself as well as key engineering/operations staff, undergo more technical continuing education.

Separation from Litmus
In the case of personnel termination or resignation, the security team coordinates with human resources to implement a standardized separation process to ensure that all accounts, credentials, and access of outgoing employees are reliably and automatically disabled.

2.4. Physical Office Environment

Access to Litmus offices require authorized electronic badges. All doors remain locked at all times under normal business conditions. The security team may provide approval to unlock doors for short periods of time in order to accommodate extenuating physical access needs.

2.5. Office Network

Internet access is provided to devices via WPA2 wifi. Networking switches and routers are placed in a locked networking closet with only the security team having access. A network firewall that blocks all WAN-sourced traffic is in place; WAN-accessible network services are not hosted within the Litmus office environment.

3. Identity and Access Management

3.1. User Accounts and Authentication

Each individual having access to any Litmus-controlled system does so via a SSO user account denoting their system identity. All Litmus user accounts are required to have a unique username, a unique password of at least 25 characters, and two-factor authentication (2FA) enabled.

Logging into Litmus Systems
Logins by personnel may originate only from Litmus-managed devices. Authentication is performed by a SSO account management system. Litmus leverages built-in services to detect malicious authentication attempts. Repeated failed attempts to authenticate may result in the offending user account being locked or revoked.

Logging into Third Party Systems
Whenever available, third-party systems must be configured to delegate authentication to Litmus's SSO account authentication system (described above) thereby consolidating authentication controls into a single user account system that is centrally managed by the security team.

Revocation and Auditing of User Accounts
User accounts are revoked (i.e. disabled but not deleted) immediately upon personnel separation. As a further precaution, all user accounts are audited at least quarterly, and any inactive user accounts are revoked.

3.2. Access Management

Litmus adheres to the principle of least privilege, and every action attempted by a user account is subject to access control checks.

Role-based Access Control
Litmus employs a role-based access control (RBAC) model utilizing AWS identity and access management services.

Web Browsers and Extensions
Litmus may require use of a specified web browser(s) for normal business use and for access to corporate data such as email. For certain specified roles such as software development and web design, job activities beyond those mentioned above necessitate the use of a variety of browsers, and these roles may do so as needed for those activities.

Administrative Access

Access to administrative operations is strictly limited to appropriate team members and further restricted still as a function of tenure and the principle of least privilege.

Regular Audit

Access control policies are reviewed regularly with the goal of reducing or refining access whenever possible. Changes in job function by personnel trigger an access review as well.

3.3. Termination

Upon termination of personnel, whether voluntary or involuntary, the applicable personnel exit procedures are followed, which includes revocation of the associated user account and reclamation of company-owned devices, office keys or access cards, and all other corporate equipment and property prior to the final day of employment.

4. Engineering and Technical Operations

4.1. Software Development Lifecycle

Litmus stores source code and configuration files in private GitHub repositories. The security and development teams conduct code reviews and execute a static code analysis tools on every code commit. Reviewers check for compliance with Litmus's conventions and style, potential bugs, potential performance issues, and that the commit is bounded to only its intended purpose.

Security code reviews are conducted on every code commit to security-sensitive modules. Such modules include those that pertain directly to authentication, authorization, access control, security logging, and encryption.

All major pieces of incorporated open source software libraries and tools are reviewed for robustness, stability, performance, security, and maintainability.

The security and development teams must establish and adhere to a formal software release process.

4.2. Configuration and Change Management

The Litmus security and development teams must document the configuration of all adopted systems and services, whether hosted by Litmus or are third party hosted. Industry best practices and vendor-specific guidance are identified and incorporated into system configurations. All configurations are reviewed on at least an annual basis. Any changes to configurations must be approved by appointed individuals and documented in a timely fashion.

System configurations must address the following controls in a risk-based fashion and in accordance with the remainder of this policy:

- Data-at-rest encryption
- Data-in-transit protection of confidentiality, authenticity, and integrity for incoming and outgoing data
- Data and file integrity
- Malware detection and resolution
- Capturing event logs
- Authentication of administrative users
- Access control enforcement
- Removal or disabling of unnecessary software and configurations
- Allocation of sufficient hardware resources to support loads that are expected at least twelve months into the future.

4.3. Third Party Services

For every third-party service that Litmus adopts, the security team reviews the service and vendor, on an annual basis, to gain assurance that their security posture is consistent with Litmus's for the type and sensitivity of data the service will store.

5. Data Classification and Processing

5.1. Data Classification

Litmus maintains the following classes and processing rules of customer data. For each data class, the Litmus security and development teams must provision and dedicate specific information systems in AWS to store and process data of that class, and only data of that class, unless otherwise explicitly stated throughout Section 5. For all classes of customer data, the corresponding systems may store and process data items needed to keep each customer's data properly segmented, such as Litmus customer identifiers.

Customer User Account Data
This is data pertaining to login accounts for the www.Litmus.com customer web interface, used by Litmus customer agents. This data is encrypted-at-rest so as to protect the data in the event of unauthorized access attempts. User account credentials are hashed in such a manner that the plaintext passwords cannot be recovered.

Customer Contact Data
This is contact data about Litmus customers and customer agents.

Customer Preferences Data
This is data pertaining to the customer-specific preferences and configurations of the Litmus service made by customer agents.

Customer Recorded Data
This is data that the Litmus service collects during session recording. The Litmus security and development teams must provision specific systems within AWS to store and process this class of data. This data is encrypted-at-rest so as to protect the data in the event of unauthorized access attempts.

Customer Event Transaction Metadata
This is metadata about transactions conducted on all other classes of customer data. This includes customer organization and user identifiers, standard syslog data pertaining to customer users, and instances of Customer Contact Data and Customer Preferences Data. This class does not include Customer Recorded Data.

Customer Contact Data, Customer Preferences Data, and Customer Event Transaction Metadata may be stored and processed in systems hosted in environments other than AWS, as approved by the security team.

5.2. Personnel Access to Customer Data

Litmus employees can access Customer Data only under the following conditions:

- From Litmus-owned and managed devices
- For the purpose of incident response, customer support, or feature testing.
- For the no longer than is needed to fulfill the purpose of access.
- In an auditable manner.

5.3. Customer Access to Customer Data

Litmus provides web user interfaces (UIs), application programming interfaces (APIs), and data export facilities to provide customers access to their data.

5.4. Exceptional Cases

The security team in conjunction with executive management may approve emergency exceptions to any of the above rules, in response to security incidents, service outages, or significant changes to the Litmus operating environment, when it is deemed that such exceptions will benefit and protect the security and mission of Litmus, Litmus customers, and visitors of Litmus customers' websites.

6. Vulnerability and Incident Management

6.1. Vulnerability Detection and Response

The Litmus security and development teams use all of the following measures to detect vulnerabilities that may arise in Litmus's information systems.

- Cross-checking vulnerability databases with all systems and software packages that support critical Litmus services.
- Automated source code scanners on every code commit.
- Code reviews on every security-sensitive code commit.
- Vulnerability scanning on Litmus services.
- Maintain a bug bounty program.
- Annual penetration testing with an independent provider.

The Litmus security team evaluates the severity of every detected vulnerability in terms of the likelihood and potential impact of an exploit, and develops mitigation strategies and schedules accordingly. Suitable mitigations include complete remediation or implementing compensating controls.

6.2. Incident Detection and Response

The Litmus security team uses all of the following measures to detect security incidents.

- Monitor logs to detect potentially malicious or unauthorized activity.
- Conduct reviews on the causes of any service outages.
- Respond to notices of potential incidents from employees, contractors, or external parties.

The Litmus security team makes a determination of whether every indicator is representative of an actual security incident. The severity, scope, and root cause of every incident are evaluated, and every incident is resolved in a manner and timeframe commensurate with the severity and scope.

In the event that a data breach affecting a customer has been detected, Litmus maintains communication with the customer about the severity, scope, root cause, and resolution of the breach.

7. Business Continuity and Disaster Recovery

Litmus services are hosted in Amazon Web Services (AWS) and are configured in such a manner in order to withstand long-term outages to the AWS-US East1 region. Controls such as automated replication and automated data recovery processes are used to achieve this desired level of availability.