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

(866) 787 7030

hello@litmus.com

Simplified Information Security Policy

Updated 5 February 2018 | security@litmus.com

Public

Revision History

Date	Version	Author	Detail
10 May 2017	0.1	Naomi Buckwalter	Initial draft.
11 May 2017	1.0	Naomi Buckwalter	Published.
18 July 2017	1.1	Naomi Buckwalter	Minor change to Security Controls - addition of Application Security; Compliance & Security Audits
5 Feb 2018	2.0	Naomi Buckwalter	Added links to Privacy Policy and Terms of Service

Executive Sign Off

Date	Name	Comments
11 May 2017	Matt Gore, VP Engineering	Reviewed and approved.

Document Owner

Name	Title	Contact
Naomi Buckwalter	Director of Information Security	naomi@litmus.com

Purpose

Litmus Software, Inc. strives to provide the best products and services to our customers, which in turn enables our customers to be successful in their business. Litmus team members live by the following creed:

1. In our people we value friendliness, approachability, and humility. We are discerning, transparent, and supportive.
2. In our work we tackle big problems with a narrow focus. We highly value design, simplicity, and attention to detail.
3. As a business we put product before financial goals. We are self-funded, profitable, and proud of that. We are only interested in building innovative, high-quality products.
4. Above all, we get things out the door and into our customers' hands.

The **Information Security Program** at Litmus provides the highest level of security, control, and transparency expected from our customers. Our **Information Security Policy** ensures the confidence of our clients and partners by providing guidance and direction for the use of information owned and controlled by Litmus.

Scope

This document contains a summary of the governance approach, roles and responsibilities, information classification, and security controls that protect Litmus, its systems, customers' systems, and customer data.

This Information Security Policy applies to all Litmus employees, contractors, agents, and affiliates.

Security Governance Approach

At Litmus, our approach to Information Security ensures that our organization aligns information security policy with business objectives at all times. All information security projects and initiatives contribute to the organization's overall success.

Roles and Responsibilities

Shared Responsibility Model

Litmus Responsibilities

Litmus Software, Inc. is responsible for the confidentiality, integrity, and availability of the Litmus Platform, its customers' data, and its underlying infrastructure. Security-related tasks include, but are not limited to: asset management, end-user security education, incident response, disaster recovery, physical security, server-level patching, endpoint protection, vulnerability management, password management and multi-factor authentication, penetration testing, network security, security event logging & monitoring, operational monitoring, and availability assurance in accordance with published SLA's.

Customer Responsibilities

The customer is responsible for the security and training of their users and the management and authorization of user accounts to their configuration of the Litmus Platform. For information on our Privacy Policy, visit https://litmus.com/privacy. For our Terms of Service, please visit https://litmus.com/terms.

Cloud Host Responsibilities

The Litmus Platform runs on the AWS and MacStadium cloud platforms. Both cloud providers are responsible for the security of their services, platform, and infrastructure. Both AWS & MacStadium maintain SSAE 16 SOC 2 compliance.

Information Classification

Information is a critical resource at Litmus. To ensure that we meet customer, industry, regulatory, and privacy standards, and to reduce the risk that restricted or sensitive information is accidentally released to unauthorized parties, we follow a structured four-tier data classification system:

1. **Public** – This information is approved for public release by our Marketing team. Disclosing this information would not be a problem for Litmus, its customers, or business partners.

2. **Internal Use Only*** – This information is intended for use within Litmus, and in some cases with other affiliated organizations, such as business partners or vendors. Unauthorized disclosure of this information may be a violation of laws and regulations or may otherwise cause problems for Litmus, its customers, or business partners.

3. **Confidential** – This information is private or otherwise sensitive in nature and is restricted to those with a legitimate business need for access. Unauthorized disclosure of this information may be against laws and regulations, or may cause significant problems for Litmus, its customers, or business partners.

4. **Secret** – This information is the most private or otherwise sensitive, and is monitored and controlled at all times. Unauthorized disclosure of this information to people without a legitimate business need for access may be against laws and regulations and will cause severe problems for Litmus, its customers, or business partners.

***** If information is not explicitly assigned a data classification (i.e. is not labeled), it is categorized *Internal Use Only* by default.

Security Controls

The following technical and administrative security controls are in place at Litmus to strengthen our security posture and maintain the highest levels of confidentiality, integrity, and availability required by the business and our customers:

Application Security	The technical and administrative controls used to protect our applications from security threats.
Asset Management	The documentation, monitoring, and reporting of Litmus assets (e.g. data, physical machines, intellectual property), their owners, classification level, and lifecycle requirements.
Compliance & Security Audits	Scheduled third-party audits of our infrastructure, code, and processes to ensure we maintain the highest level of confidentiality, integrity, and availability of our systems and data. Compliance with major national and international privacy and data protection regulations.
Disaster Recovery	The processes and procedures followed in order to ensure the overall continuation of Litmus business operations during an outage event.
Endpoint Protection	The hardening, patching, and protection of endpoints used by Litmus employees and contractors.
Network Security	The configuration and application of security controls as applied to network devices to prevent unauthorized access or incorrect updates to the Litmus network.
Password Management and Multi-factor Authentication	The policies, procedures, and technical guidelines that ensure the secure implementation of the password management lifecycle at Litmus, as well as the guidelines and best practices for enabling multi-factor authentication for services used by Litmus team members.
Physical Security	The policies, procedures, and best practices that ensure the physical protection of Litmus assets against accident, attack, or unauthorized physical access.
Security Awareness Training	Activities undertaken by Litmus employees to ensure that effective, risk-based decisions are made in the best interest of the organization, while protecting critical and sensitive information from being compromised.
Security Event Logging and Monitoring	The recording, storage, and monitoring of important security-related events to help in the identification of threats that may lead to an information security incident, and to support forensic investigations.

Security Response	The identification and resolution of information security incidents quickly and effectively, minimizing their impact to the business, and reducing the risk of similar incidents occurring in the future.
Vulnerability Management	The standards and procedures for the identification and remediation of Litmus system and software security vulnerabilities.