Approval Signature Dayle Alsbury **Date Approved** 02-Aug-2023

Name and title Dayle Alsbury, VP Information Security; Information Security Officer

Change history

Date	Version	Created by	Description of change
14-Jun-23	1.0	J. Clayton	Initial document creation
21-Jun-23	1.1	D. Alsbury	ISO approved and finalized
02-Aug-23	1.2	D. Alsbury	Addition to 14.2.6

The following sections define Litmos' current technical and organizational measures and are incorporated into Schedule 3 of the DPA. Litmos may change these at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data (sensitive or restricted data, as defined by Litmos Data Classification Standards.).

Litmos – Litmos' Learning Management System ("**Company**") monitors the application in the customer's portfolio; Company automatically monitors and correlates together three streams of data – user interactions, device health, and application performance, as seen by the end user.

The Company Agent transmits Customer Data to Company servers, where it is processed, and end user analytics are displayed back to the customer.

1 SECURITY POLICY

1.1 Litmos has a set of information security policies approved by management, published, and communicated to relevant Company personnel.

1.2 Litmos undergoes an independent evaluation in the form of an annual SOC 2 Type 2 audit report; a copy is available upon request.

2 CLOUD ARCHITECTURE AND SECURITY

2.1 The Company uses AWS Elastic Compute cloud services for third party hosting of servers and equipment in an Infrastructure-as-a-Service environment including the restriction of physical access, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

2.2 The Company uses AWS' Relational Database Services (RDS) as a Database-as-a-Service.

2.3 The Company uses Microsoft Azure's (Azure) Platform-as-a-Service for its third-party hosting of servers and equipment, including the restriction of physical access, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.

2.4 The Company uses Microsoft Azure Directory Software-as-a-Service.

2.5 The Company has key operations and stores Customer Data in cloud data centers in the following locations:

2.5.1 Frankfurt, Germany – Amazon Web Services (Europe)

2.5.2 Sydney, Australia - Amazon Web Services (Asia Pacific)

2.5.3 Virginia, USA – Microsoft Azure (US East)

2.6 Company's cloud environment has the following control capabilities in place:

2.6.1 Antivirus / antimalware

2.6.2 Firewalls

2.6.3 Logging, intrusion detection, monitoring, & alerting

2.6.4 Multifactor authentication

2.6.5 Security incident response

2.7 Company cloud data center resources are architected to prevent data transfer risk by utilizing hardened 'jump boxes' to span dissimilar regional security zones and provide secure remote regional data center access to process necessary support functions following established Change Management.

2.7.1 Litmos technical support personnel may use virtual access (via hardened virtual jump boxes) systems outside the data hosting region to satisfy contractual support and availability requirements. The hardened virtual jump boxes prevent data storage from occurring outside the dedicated hosting region.

2.7.2 Litmos support personnel outside the dedicated hosting region may use limited customer and end-user contact information, such as name, email address, and/or phone number when assisting with email delivery support issues to satisfy contractual support and availability requirements.

3 COMPANY PERSONNEL ACCESS CONTROL

3.1 Company has an access control program that has been approved by management and communicated to relevant Company personnel. Company product management is responsible for ownership and regular review of the Company's access control program.

3.2 Company uses a central identity and access management system to provision access by Company personnel in accordance with the principle of least privilege.

3.3 Individual IDs are required for user authentication to Company systems.

3.4 Segregation of duties is considered for approving and implementing access requests.

3.5 User access rights are reviewed at least quarterly.

3.6 Access rights are reviewed when a Company employee changes roles.

3.7 Privileged user access reviews are conducted at least annually.

3.8 All privileged account activities are logged and monitored.

3.9 Only a select predefined group of users are granted privileged system administration accounts: operations staff and SaaS admin users; each action taken by system administrators is audited. On a weekly basis, the Company team reviews any activities requiring privilege administrative access and ensures such activities were undertaken by authorized users.

3.10 Multi-factor authentication is deployed for both remote access (VPN) and privileged accounts (admin).

3.11 Shared user account credentials are securely stored, and access is controlled, audited and monitored.

3.12 Remote sessions timeout after a thirty (30) minute period.

3.13 Company personnel are required to use passwords that include:

3.13.1 A minimum password length of at least eight characters.

3.13.2 A requirement of complexity (a combination of upper-case letters, lower case letters, numbers and special characters).

3.13.3 Password history at least 12 before reuse.

3.13.4 A requirement for initial and temporary passwords to be changed upon next login.

3.13.5 A requirement that initial and temporary passwords be random and complex.

3.13.6 A requirement to change passwords when there is an indication of possible system or password compromise.

3.13.7 A requirement that passwords expire periodically.

3.13.8 A requirement to terminate or secure active sessions when finished.

3.13.9 A requirement to log off terminals, PC or servers when the session is finished.

3.14 A requirement to not include unencrypted passwords in automated logon processes.

3.15 Passwords are encrypted in transit.

3.16 Passwords are encrypted or hashed in storage.

3.17 Encrypted communications are required for all remote connections.

4 APPLICATION SECURITY

4.1 Development, Test and Staging environments are separated from the Production environment by either separate VPC, Availability Zone or physical location.

4.2 Company utilizes a formal Software Development Life Cycle (SDLC) process that has been approved by management and communicated to appropriate Company personnel. The Company product management team is responsible for maintaining and reviewing the SDLC policy.

4.3 Company maintains a documented change management / change control process that includes:

4.3.1 Change control procedures required for all changes to the production environment.

4.3.2 Testing prior to deployment.

4.3.3 Stakeholder communication and/or approvals.

4.3.4 Documentation for all system changes.

4.3.5 Logging of all change requests.

4.3.6 Backout procedures are required for production changes.

4.3.7 Secure coding requirements

4.3.8 Access to make changes to source code is restricted to select Company personnel.

4.4 Product platform software is evaluated from a security perspective prior to promotion to production.

4.5 For every release, the following security testing procedures are performed:

4.5.1 Security architecture review.

4.5.2 Secure code reviews.

4.5.3 Vulnerability scans.

4.5.4 Company is subject to third party penetration testing at least annually.

4.5.5 Company conducts regular vulnerability analysis.

5 ASSET AND INFORMATION MANAGEMENT

5.1 Company maintains and periodically reviews an asset management program approved by management that is communicated to relevant Company personnel; the asset management program includes an asset inventory list.

5.2 A process is in place to verify the return of Company personnel assets (e.g., computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination.

5.2.1 Company personnel must return assets as soon as possible and access to Company systems is revoked immediately upon termination.

5.2.2 Company employs Data Loss Prevention and conditional access technologies to protect customer & sensitive information.

5.3 Company does not send or receive Customer Data via physical media.

5.4 For Customer Data sent or received electronically, Company encrypts Customer Data both in transit while outside the network and within the network.

5.5 Company utilizes current supported cryptographic technologies & standards to protect data at rest and data in transit.

5.5.1 For Customer Data stored electronically, Company:

5.5.1.1 Encrypts Customer Data at rest using AWS & Azure key management and AES (Advanced Encryption Standards) 256-bit encryption.

5.5.1.2 Enables full-disk encryption.

5.6 Company manages and maintains encryption keys in accordance with key management industry standards.

6 INFORMATION HANDLING

6.1 Company classifies data according to legal or regulatory requirements and sensitivity to unauthorized disclosure and/or modification using a defined Data Classification Standard.

6.2 Litmos disposes of confidential data from the Litmos environment internally through secure disposal mechanisms and guidance provided in NIST Special Publication 800-88; Guidelines for Media Sanitization. Customer confidential data is disposed of in conformance with relevant regulations, contractual requirements, or as required by customers.

6.3 Data may be disposed of using certified commercial disposal vendors. Where an external disposal vendor is utilized, the disposal vendor shall provide a certificate of destruction, which includes description and date of disposal.

7 OPERATIONS MANAGEMENT

7.1 Company maintains and periodically reviews a documented operational change management / change control program that has been approved by management and communicated to relevant Company personnel.

7.2 Changes to the production environment including systems, application updates and code changes are subject to the change control process.

8 END USER DEVICE SECURITY

8.1 Company does not use End User Devices for transmitting, processing or storing Customer Data. Customer Data is transmitted from the Company Agent to Company servers for processing and storage; these servers are hosted on cloud infrastructure.

8.2 Company utilizes end user device security technologies to detect and prevent malware, viruses, and suspicious behavior.

9 NETWORK SECURITY

9.1 Company is hosted on cloud infrastructure and as such cloud infrastructure providers are responsible for all network management.

10 HUMAN RESOURCE SECURITY

10.1 Company maintains a set of human resource policies that have been approved by management, published, and communicated to all Company personnel. A disciplinary process is in place for non-compliance.

10.2 All Company personnel are required to undergo background screening, which includes a criminal background check, prior to commencing employment.

10.3 All Company personnel are required to enter into employment agreements including provisions relating to acceptable use, code of conduct/ethics, and confidentiality.

10.4 All Company personnel must undergo annual security training. Select roles are required to undergo additional security training.

10.5 Access to Company systems containing Customer Data is centrally managed and revoked immediately upon termination.

11 ORGANIZATIONAL SECURITY

11.1 Company has designated an individual responsible for information security within its organization (the "**Information Security Officer**") and has defined information security roles and responsibilities throughout the organization. Internal information security personnel are responsible for corporate information security processes.

11.2 All Company personnel are required to undergo annual security training in addition to Company's ongoing security awareness program.

11.3 Company product management oversees the product-specific security program and features.

12 LOGGING AND THREAT MANAGEMENT

12.1 Company maintains and periodically reviews its anti-malware program; the anti-malware program has been approved by management and communicated to relevant Company personnel.

12.2 Company maintains and periodically reviews its vulnerability management program; the vulnerability management program has been approved by management and communicated to relevant Company personnel.

12.2.1 System vulnerability reviews are conducted on a monthly basis.

12.2.2 Code application security vulnerability scans are performed as part of the software delivery process.

12.2.3 On at least an annual basis, an independent consulting firm executes an application penetration test and an external penetration test against the in-scope Company Cloud Service assets.

12.3 Vulnerabilities are assessed and assigned a rating based on guidance from the Common Vulnerability Scoring System (CVSS), where applicable.

12.3.1 Litmos has established system vulnerability response and remediation timelines which are aligned with severity levels

12.3.2 The remediation of application vulnerabilities follows Litmos Change Management controls and is aligned to the relevant risk exposure. Application remediation times may differ from system remediation times as necessary.

12.4 Logs ensure that the actions of individual information system users can be uniquely traced to user activity. Event logs, where applicable, should include relevant user, device, & system activity event information.

12.4.1 Additional event information or attributes may be included, as necessary and/or appropriate such as user privilege changes, data access or interaction, network traffic data, systems utilities logs, internet communications logs, and/or service provider logs, where supported.

13 INCIDENT EVENT AND COMMUNICATIONS MANAGEMENT

13.1 Company has an established incident management program that has been approved by management and communicated to relevant Company personnel.

13.1.1 Company's incident management program leverages a centralized incident management tool.

13.2 Company maintains formal incident response and crisis communications plans which include guidance for:

13.2.1 Feedback and lessons learned.

13.2.2 Applicable data breach notification requirements (including notification timing).

13.2.3 Escalation procedure.

13.2.4 Communication timelines and process.

13.2.5 Chain of custody for evidence during incident investigation.

13.2.6 Actions to be taken in the event of a Security Incident.

13.3 Testing of Company incident response plan occurs at least annually and includes:

13.3.1 Security incident response and data breach response.

13.3.2 Associated BCP (Business Continuity Plan) / DR (Disaster Recovery) plans.

13.3.3 Review of the test result by product management leadership and remediation if needed.

13.4 Company notifies customers of (a) Security Incidents as required by applicable law; and (b) Personal Data Breaches without undue delay as defined in the Litmos Data Processing Addendum.

14 DATA PRIVACY

14.1 **Data Collection and Processing**. Company collects anonymized regional location data not associated with the specific user.

14.2 **Personal Data**. The Descriptive Data processed by Company contains Personal Data. As of this document's publication date, Company collects and processes the following categories of Personal Data:

14.2.1 Email address

14.2.2 Name

14.2.3 Phone number

14.2.4 IP (Internet Protocol) Address

14.2.5 Special categories of personal data: Training data, completions, skills, certificates, attendance.

14.2.6 End-users may choose to include additional data at their discretion such as profile pictures, images, videos content, etc.

14.3 **Customer Data Storage**. See Section 2: (Cloud Architecture and Security).

14.3.1 Company cloud resources are architected to prevent data transfer risk by utilizing hardened 'jump boxes' to span dissimilar regional security zones and provide secure remote regional data center access to process necessary support functions following established Change Management.

14.3.2 **International Transfers of Personal Data**. Company complies with applicable data protection laws governing the transfer of Personal Data outside of the European Economic Area ("**EEA**") as further described in Company's DPA.

14.4 **Customer Data Retention**. During the contract, Customer controls data retention and may delete data manually, via API (Application Programming Interface), or by using the data retention scheduling tools.

14.4.1 Any Personal Data processed by the Company is retained for no longer than three (3) months after contract termination, after which period it is deleted, as defined in the Litmos Data Processing Addendum.

14.5 **Subprocessors.** Company assesses the privacy and security practices of any Subprocessor engaged by Company to assist with the processing of Customer Data. Subprocessors are required to enter into appropriate security, confidentiality and privacy contract terms with the Company based on the risks presented by the assessment, including data processing terms as required by applicable law.

14.5.1 The list of company Subprocessors is located at https://www.litmos.com/termsandconditions

15 BUSINESS CONTINUITY, DATA BACKUP AND DISASTER RECOVERY

15.1 The Company establishes production platform fault tolerance by implementation of supporting infrastructure across at least two cloud infrastructure availability zones for both the AWS and Azure production environments.

15.1.1 Backups are configured to automatically protect backup of production data utilizing Advanced Encryption Standards (AES).

15.1.2 Production environment databases are configured to synchronize across production nodes continuously.

15.1.3 Controls over the underlying data centers infrastructure, including safeguards such as UPS (Uninterruptible Power Supply), backup generators, and hardware redundancy are the responsibility of AWS and Microsoft (Azure).

15.1.4 Company has a Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DR")

15.1.4.1 The BCP & DR plans are validated on an annual basis.

15.1.5 Company has defined Recovery Time Objectives ("**RTO**") and Recovery Point Objectives ("**RPO**") as part of the Disaster Recovery Plan.

15.1.6 Company DR tests on a regular basis to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing Company's DR procedures.

16 SUPPLEMENTAL DOCUMENTATION

16.1 A copy of the Litmos SOC 2 Type 2 report is available upon request. Terms & Conditions, Data Processing Addendum, and other documentation are available at https://www.litmos.com/termsandconditions

17 Definitions

Process Term / Acronym	Definition / Explanation
Company Agent	An application or device that transmits Customer Data to Company.
AWS	Amazon Web Services
Azure	Microsoft Azure Cloud Services
End User Devices	Company-managed desktops, laptops, tablets and smartphones.
Personal Data	Any information related to an identified or identifiable natural person.
Personal Data Breach	A subtype of Security Incident involving Personal Data
Security Incident	A breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed or otherwise controlled by Company. "Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.