

Information Security Addendum

This Addendum forms part of the applicable agreement between Systemslab and Customer governing the Systemslab Offerings (the “Agreement”). It sets out the security measures Systemslab shall maintain for Customer Information processed in connection with those Offerings. Capitalised terms not defined here have the meanings given in the Agreement or DPA.

Customer Information includes Customer Content and Customer Personal Data processed by Systemslab. These obligations apply to systems and processing under Systemslab’s control, including its handling of support information for on-premises deployments. Customer remains responsible for its own infrastructure and controls as described in Section 7.

1 Security programme

Systemslab shall maintain a written security programme covering the confidentiality, integrity, availability and resilience of Customer Information and the systems processing it. The programme shall include assigned responsibilities, documented policies, risk assessment, control review and corrective actions proportionate to the service and processing risks.

Management shall review the programme and material security risks at least annually and following material changes or incidents. Systemslab may replace individual controls with measures serving the same protective purpose, provided that the change does not materially reduce the overall protection or any express contractual commitment. Changes remain subject to the Agreement and applicable law.

2 Access and technical safeguards

2.1 Access control and authentication

Systemslab shall restrict access to Customer Information to authorised personnel with a legitimate business need. Human accounts shall be individually assigned, approved before access is granted and limited according to role and least privilege. Access shall be reviewed at least annually and promptly removed when no longer required, including after a role change or departure.

Multi-factor authentication shall be enforced for human privileged administrative access to Systemslab-controlled production systems and repositories containing Customer Information. Service accounts shall use restricted permissions and securely managed credentials. Emergency access shall be controlled, logged and reviewed after use. Authorised support-provider access shall be subject to equivalent access restrictions.

2.2 Encryption and key management

Systemslab shall encrypt Customer Information transmitted over public networks using industry-recognised secure protocols. Stored Customer Information within Systemslab-controlled UXM SaaS production databases, storage and backups shall be encrypted at rest. Cryptographic keys and other secrets shall be protected against unauthorised access, with access restricted to authorised roles.

Customer Information in support repositories and export files shall be protected by appropriate encryption and access controls. Encryption coverage, key-management responsibilities and any legally permissible technical exceptions shall be documented. Ordinary email delivery does not provide a guarantee of end-to-end encryption; alert content shall be limited to information necessary for the configured purpose.

2.3 Logging and monitoring

Systemslab shall log relevant privileged administrative activity and security events in systems under its control, including authentication events and material access or configuration changes. Relevant logs shall be protected from unauthorised modification and deletion and retained under a documented retention policy.

Systemslab shall operate service and security monitoring, with alerts directed to personnel responsible for assessment and escalation. Monitoring coverage, operational response arrangements and log-retention periods shall be documented. This clause does not create a separate round-the-clock staffed monitoring or incident-response service commitment.

2.4 Vulnerability management

Systemslab shall maintain a documented process to identify, assess and remediate vulnerabilities in the software and infrastructure under its control. The process shall include vulnerability scanning, dependency review, patch management and security testing appropriate to the service. Findings shall be prioritised according to severity, exploitability, exposure and the potential effect on Customer Information.

Remediation targets, responsibility, escalation and approved exceptions shall be documented. Systemslab shall track corrective actions and verify remediation. Independent penetration testing shall be performed on a documented, risk-based schedule; scope, frequency and follow-up shall be recorded.

2.5 Secure development

Systemslab shall restrict source-code access, control production changes and test material changes before deployment. Development practices shall include code review, dependency management and security review appropriate to the change.

3 Personnel suppliers and physical security

Personnel with access to Customer Information shall be bound by confidentiality obligations and receive security and privacy instruction appropriate to their duties at onboarding and at least annually. Systemslab shall maintain appropriate protection for personnel devices used to access Customer Information, including access restrictions, device encryption and protective software appropriate to the device and risk. Screening shall be conducted where appropriate and lawful.

Systemslab shall assess material providers that process Customer Information or support service delivery, considering the nature of access, security safeguards, relevant assurance evidence and contractual obligations. Provider access shall be limited to the authorised purpose. Processing of Customer Personal Data, subprocessor changes and transfers remain governed by the DPA and Annex III.

For facilities directly controlled by Systemslab, physical access shall be restricted to authorised persons. Physical security of third-party hosting facilities shall be provided by the hosting provider and assessed through relevant assurance evidence. A provider's certification does not constitute a certification of Systemslab.

4 Backup recovery and continuity

Systemslab shall maintain documented backup and recovery procedures for UXM SaaS, covering the data and configurations required for restoration. The procedures shall specify backup frequency, retention, access protection, monitoring of backup success and internal recovery objectives. Restore procedures shall be tested at least annually and following material changes where necessary, with results and corrective actions recorded.

UXM SaaS application data, including all replicas, and backups shall remain within the Customer-selected region recorded in the Order Form. Systemslab shall not replicate UXM application data or backups outside the Customer-selected region. UXM application workloads operate within the selected region. This regional location commitment does not itself represent geographic redundancy. Authorised employee remote operational access is governed by DPA Section 6.1; Google Cloud processing and other authorised supplier access remain governed by DPA Sections 5 and 6 and Annex III.

Specific availability commitments are governed by the applicable Service Level Agreement. Internal recovery objectives do not constitute a guaranteed recovery time or recovery point unless expressly agreed with Customer. Return, retrieval, retention and deletion are governed by the Subscription Agreement and DPA; routine backup retention shall not override a mandatory deletion obligation.

5 Security incident handling

Systemslab shall maintain documented procedures for detecting, classifying, escalating, investigating and containing security incidents, protecting relevant evidence, applying corrective actions and reviewing lessons learned. Responsibility for response and Customer communication shall be assigned, with arrangements for cover and escalation.

Upon becoming aware of a Security Breach affecting Customer Information, Systemslab shall notify Customer without undue delay. A Security Breach means a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Information for which Systemslab is responsible under the Agreement. Personal Data Breach notifications shall comply with DPA Section 4 and Applicable Data Protection Laws; notification shall not await a completed root-cause investigation.

Notification shall be sent to Customer's designated security contact or, if none is designated, its primary technical contact. The initial notice shall include the information reasonably available about the breach, affected information, likely consequences, response measures and a follow-up contact. Further information shall be provided in phases without undue further delay. Systemslab shall reasonably cooperate with Customer in investigation and mitigation. Notification does not constitute an admission of fault or liability. Customer may report security concerns to legal@uxmapp.com.

6 Assurance and Customer assessments

Systemslab shall retain appropriate records demonstrating operation of its security programme and reasonably cooperate with Customer's legitimate security assessments. Upon reasonable written request, Systemslab may provide relevant control descriptions, completed questionnaires, policy summaries and available independent assessment or test summaries, subject to confidentiality and reasonable safeguards for sensitive security information.

Routine requests shall ordinarily occur no more than once in any twelve-month period. This limitation does not restrict DPA audit rights, requests required by applicable law or a competent authority, or reasonable additional requests following a material security incident. Any restriction on sensitive disclosure shall preserve the information and audit rights required by the DPA and applicable law.

References to ISO/IEC 27001, SOC 2 or other standards are not representations that Systemslab holds a certification or audit report. Systemslab is not required to obtain a particular certification or independent audit unless expressly agreed in writing. Evidence of certification shall be provided only where current and applicable.

7 Customer responsibilities

Customer shall manage its users and access rights, protect credentials, configure Customer-controlled integrations and connections securely, and maintain security of its endpoints and infrastructure. For on-premises deployments, Customer is responsible for hosting, operating-system and database administration, network protection, backup and recovery of its environment, and applying available updates, except to the extent Systemslab expressly accepts a responsibility in the applicable Customer Order Form or service scope.

Customer responsibilities do not reduce the security, backup, availability or recovery obligations expressly undertaken by Systemslab. Services independently provided by a Reseller are governed by Customer's agreement with that Reseller and do not authorise the Reseller to access Customer Information on Systemslab's behalf.

8 Relationship with the Agreement

This Addendum shall be read with the Subscription Agreement, DPA, Service Level Agreement and Support Services Policy. Subscription Agreement Section 30.6 governs document priority and negotiated deviations. Mandatory transfer clauses retain their priority; the DPA governs conflicts concerning Customer Personal Data. This Addendum supplements DPA Annex II and does not reduce its safeguards or Customer's mandatory rights.