Origen Technologies Information Security Addendum

Origen Technologies Information Security Addendum

(For Use with On-Premises Products Only)

This Information Security Addendum ("**ISA**") sets forth the administrative, technical, and physical safeguards Origen Technologies takes to protect Confidential Information as part of its Information Security Program ("**ISP**"). Origen Technologies may update this ISA from time to time to reflect changes in Origen Technologies' ISP, provided such changes do not materially diminish the level of security herein provided.
This ISA is made a part of your Origen Technologies General Terms ("**Agreement**") with Origen Technologies. Any capitalized terms used, but not defined herein, shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this ISA, the terms of this ISA will apply. This ISA does not apply to Third-Party Content purchased or acquired through Origen Technologies.com, to any Evaluation or Free Software, or to any Extensions.
Origen Technologies' Hosted Services (including without limitation Origen Technologies' hybrid services, which are cloud enabled Offerings for On-Premises Products) include their own security provisions as applicable. Please reference the Specific Hosted Services Terms and Origen Technologies Protects for security information regarding Hosted Services. This ISA does not apply to the security of Hosted Offerings.
During the Term of the Agreement, Origen Technologies agrees to maintain an ISP in conformance with the requirements set forth below.

1. Origen Technologies' Information Security Program and Security Program Office

1. Origen Technologies' ISP is reasonably designed to help protect the confidentiality, integrity, and availability of Confidential Information against any anticipated threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction, or damage.
2. Origen Technologies' ISP contains technical and organizational measures that are appropriate to: (i) the nature, size, and complexity of Origen Technologies' business; (ii) the resources available to Origen Technologies; (iii) the type of information that Origen Technologies stores; and (iv) the need for security and confidentiality of such information.
3. Origen Technologies' Chief Information Security Officer leads Origen Technologies' ISP and develops, reviews, and approves (together with other stakeholders, such as Product Security, Legal and Internal Audit) Origen Technologies Security Policies (as defined below).

2. Security Policies and Procedures

1. Origen Technologies maintains information security, use and management policies (collectively "**Security Policies**") designed to educate employees and contractors regarding appropriate use, access to and storage of Confidential Information; restrict access to Confidential Information to members of Origen Technologies' workforce who have a "need to know" such information; prevent terminated employees from accessing Origen Technologies information and information systems post-termination; and imposing disciplinary measures for failure to abide by such policies. Origen Technologies performs background checks of its employees at time of hire,

as permitted by law. Where feasible and as applicable, Origen Technologies endeavors to align its Security Policies to ISO 27001 level standards for information security.

2. Origen Technologies Security Policies are available to employees via the corporate intranet. Origen Technologies reviews, updates, and approves Security Policies once annually to maintain their continuing relevance and accuracy.

3. Security Training and Awareness

New employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Security Policies, as well as other corporate policies, such as the Origen Technologies Code of Conduct. This includes requiring Origen Technologies employees to annually re-acknowledge the Code of Conduct and other Origen Technologies policies as appropriate. Origen Technologies conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace.

4. Logical Access Controls

Origen Technologies employs monitoring and logging technology to help detect and prevent unauthorized access attempts to its networks and production systems. Origen Technologies' monitoring includes a review of changes affecting systems' handling authentication, authorization, auditing, and privileged access to Origen Technologies production systems. Origen Technologies uses the principle of "least privilege" (meaning access denied unless specifically granted) for access to customer data.

5. Threat and Vulnerability Management

1. As part of its threat and vulnerability management program ("**TVM**"), Origen Technologies:
    i. monitors for vulnerabilities in supported versions of the Software that are acknowledged by vendors, reported by researchers, or discovered internally.
    ii. verifies vulnerabilities, rates them according to industry-standard ratings systems, and identifies them for mitigation or fixes based on severity level.
    iii. issues mitigations or fixes in minor and major product releases, as part of its maintenance program, which may include cumulative fixes for certain vulnerabilities; and
    iv. makes reasonable efforts to expedite maintenance releases for supported versions that may be affected in the case of critical risk and high impact vulnerabilities.
2. Origen Technologies regularly performs vulnerability scans and addresses detected vulnerabilities on a risk basis.
3. Incident Response Plan and Breach Notification includes procedures to be followed in the event of an actual or potential security breach, including: (i) an internal incident response team with a response leader; (ii) an investigation team performing a root cause analysis and identifying affected parties; (iii) internal reporting and notification processes; documenting responsive actions and remediation plans; and (iv) a post-incident review of events.

4. For Customers located outside the US, Origen Technologies provides notice without undue delay after becoming aware of a Data Breach. Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data as defined under the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") while being transmitted, stored, or otherwise processed by Origen Technologies. If Customer reasonably determines notification is required under GDPR, Origen Technologies will provide reasonable assistance to the extent required, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.

6. **For Customers located within the US,** Origen Technologies provides notice of a breach of Personal Information, Storage and Transmission Security
Technical security measures to guard against unauthorized access to Customer data that is being transmitted over a public electronic communications network or stored electronically.

7. **Secure Disposal**
Policies and procedures regarding the disposal of tangible and intangible property containing Customer Confidential Information so that wherever possible, Customer Confidential Information cannot be practicably read or reconstructed.

8. **Risk Identification and Assessment**
Origen Technologies employs a risk assessment program to help it reasonably identify foreseeable internal and external risks to Origen Technologies' information resources and determine if its existing controls, policies, and procedures are adequate to address the identified risks.

9. **Secure Development**
   i. Origen Technologies' Software Development methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components.
   ii. For major product releases, Origen Technologies uses a risk-based approach when applying its standard methodology, which may include such things as performing security architecture reviews, open-source security scans, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Origen Technologies performs security code review for critical features if needed; and performs code review for all features in the development environment. Origen Technologies scans packaged software to verify it's free from trojans, viruses, malware, and other malicious threats.
   iii. Origen Technologies utilizes a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized employees.

10. **Vendors**
Third-party vendors (collectively, "**Vendors**") with access to Confidential Information are subject to contractual obligations of confidentiality and risk assessments to gauge the sensitivity of information being shared. Vendors are expected to comply with any pertinent contract terms relating to the security of data, as well as any applicable Origen Technologies policies or procedures.

Periodically, Origen Technologies may ask the Vendor to re-evaluate its security posture to help ensure compliance.