ORIGEN CLOUD SOLaaS (Solution as a Service) SECURITY ADDENDUM

ORIGEN CLOUD SOLaaS
(Solution as a Service) SECURITY ADDENDUM

This Origen Cloud SOLaaS Security Addendum (CSA) sets forth the administrative, technical, and physical safeguards Origen takes to protect Confidential Information, including Customer Content, in Origen Cloud SOLaaS (Security Program). Origen may update this CSA from time to time to reflect changes in Origen's security posture, provided such changes do not materially diminish the level of security herein provided.

This CSA is made a part of your Origen General Terms (Agreement) with Origen and any capitalized terms used but not defined herein shall have the meaning set forth in the Agreement or Documentation, as applicable. In the event of any conflict between the terms of the Agreement and this CSA, this CSA will control.

1. Purpose

1.1 This CSA describes the information security standards that Origen maintains to protect Confidential Information, including Customer Content, in addition to any requirements set forth in the Agreement.
1.2 The CSA is designed to protect the confidentiality, integrity, and availability of Confidential Information, including Customer Content, against anticipated or actual threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction, or damage in accordance with laws applicable to the provision of the Service.

2. Origen Security Program

2.1 Scope and Content. Origen Security Program: (a) complies with industry recognized information security standards; (b) includes administrative, technical, and physical safeguards designed to protect the confidentiality, integrity and availability of Confidential Information, including Customer Content; and (c) is appropriate to the nature, size, and complexity of Origen's business operations.
2.2 Security Policies, Standards and Methods. Origen maintains security policies, standards, and methods (collectively, Security Policies) designed to safeguard the processing of Confidential Information, including Customer Content, by employees and contractors in accordance with this CSA.
2.3 Security Program Office. Origen's Chief Information Security Officer (CISO) leads Origen's Security Program and the CISO Office develops, reviews, and approves, together with appropriate stakeholders, Origen's Security Policies.
2.4 Security Program Updates. Origen Security Program Policies are available to employees via the corporate intranet. Origen reviews, updates, and approves Security Policies annually to maintain their continuing relevance and accuracy. Employees receive information and education about Origen's Security Policies during onboarding and annually thereafter.
2.5 Security Training & 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 Origen's Security Policies, as well as other corporate policies, such as the Origen Code of Conduct. This includes requiring Origen employees to annually re-acknowledge the Code of Conduct and other Origen policies as appropriate. Origen conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace.

3. Risk Management

3.1 Origen manages cybersecurity risks in accordance with its Risk Assessment Method, which defines how Origen identifies, prioritizes, and manages risks to its information assets and the likelihood and impact of them occurring.
3.2 Origen management reviews documented risks to understand their potential impact to the business, determine appropriate risk levels and treatment options. Mitigation plans are implemented to address material risks to business operations, including data protection.

4. Change Management

4.1 Origen deploys changes to the Services during maintenance windows, details of which are posted to the Origen website or communicated to customers as set forth in the Origen Cloud SOLaaS Service Maintenance Policy
4.2 Origen follows documented change management policies and procedures for requesting, testing and approving application, infrastructure, and product related changes.
4.3 Changes undergo appropriate levels of review and testing, including security and code reviews, regression testing and user acceptance prior to approval for implementation.
4.4 Software development and testing environments are maintained and logically separated from the production environment.

5. Incident Response and Breach Notification

5.1 Origen has an incident response plan (the Origen Incident Response Framework or SIRF) and team to assess, respond, contain, and remediate (as appropriate) identified security issues, regardless of their nature (e.g., physical, cyber, product). Origen reviews and updates the SIRF annually to reflect emerging risks and "lessons learned."
5.2 Origen notifies Customers without undue delay after becoming aware of a Data Breach. As used herein, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Content under the applicable Agreement, including Personal Data while being transmitted, stored, or otherwise processed by Origen.
5.3 In the event of a Data Breach involving Personal Data, if a customer determines notification is required by law, Origen will provide reasonable assistance to the extent required for the Customer to comply with applicable data breach notification laws, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.
5.4 In the event of a conflict between the breach notification provisions in this CSA and those set forth in an applicable Business Associate Agreement (BAA) with Origen, the BAA breach notification terms will apply.

6. Governance and Audit

6.1 Origen conducts internal control assessments on an ongoing basis to validate those controls are designed and operate effectively. Issues identified from assessments are documented, tracked, and remediated as appropriate.
6.2 Third party audits are performed as part of our certification process (further below) to validate the ongoing governance of control operations and their effectiveness. Issues identified are documented, tracked, and remediated as appropriate.

7. Access and User Management

7.1 Origen implements reasonable controls to manage user authentication for employees or contractors with access to Customer Content, including without limitation, assigning each employee or contractor with unique and/or time limited user authorization credentials for

access to any system on which Customer Content is accessed and prohibiting employees or contractors from sharing their user authorization credentials.
7.2 Origen allocates system privileges and permissions to users or groups on a "least privilege" principle and reviews user access lists and permissions to critical systems on a quarterly basis, at minimum.
7.3 New users must be pre-approved before Origen grants access to Origen corporate and cloud networks and systems. Pre-approval is also required before changing existing user access rights.
7.4 Origen promptly disables application, platform, and network access for terminated users upon notification of termination.

8. Password Management and Authentication Controls

8.1 Authorized users must identify and authenticate to the network, applications, and platforms using their user ID and password. Origen's enterprise password management system requires minimum password parameters.
8.2 Authorized users are required to change passwords at pre-defined intervals consistent with industry standards.
8.3 Key authentication and enterprise password management applications are utilized to manage access to the production environment.
8.4 Two-factor authentication (2FA) is required for remote access and privileged account access for Customer Content production systems.

9. Encryption and Key Management

9.1 Origen uses industry-standard encryption techniques to encrypt Customer Content
9.2 Origen relies on policy controls to help ensure sensitive information is not transmitted over the Internet or other public communications unless it is encrypted in transit.
9.3 Where applicable, Origen uses encryption at rest with a minimum encryption protocol of Advanced Encryption Standard
9.4 Origen uses encryption key management processes to help ensure the secure generation, storage, distribution, and destruction of encryption keys.

10. Threat and Vulnerability Management

10.1 Origen has a program to continuously monitor for vulnerabilities that are discovered internally through vulnerability scans, offensive exercises (red team), and employees; or externally reported by vendors, researchers, or others.
10.2 Origen documents vulnerabilities and ranks them based on severity level as determined by the likelihood and impact ratings. Origen assigns appropriate team(s) to conduct remediation and track progress to resolution as needed.
10.3 Origen conducts security penetration tests on the corporate and Origen Cloud SOLaaS environments to detect network and application security vulnerabilities. Findings from these tests are evaluated, documented, and assigned to the appropriate teams for remediation based on severity level. In addition, Origen conducts internal penetration tests on its Origen Cloud SOLaaS infrastructure and remediates findings as appropriate.

11. Logging and Monitoring

11.1 Monitoring tools and services are used to monitor systems across Origen for application, infrastructure, network, and storage events, performance, and utilization
11.2 Event data is aggregated and stored using appropriate security measures designed to prevent tampering. Logs are stored in accordance with Origen's data retention policy.
11.3 The Origen Security Team continuously reviews alerts and follows up on suspicious events as appropriate.

12. Secure Development

12.1 Origen's Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of software components.

12.2 For major and minor product releases, Origen uses a risk-based approach when applying its standard SDLC methodology, which includes such things as performing security architecture reviews, security scans, code review, dynamic application security testing, network vulnerability scans and external penetration testing. Origen performs security code review for critical features if needed; and performs code review for all features in the development environment. Origen scans packaged software to ensure it's free from trojans, viruses, malware, and other malicious threats.

12.3 Origen 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.

13. Network Security

13.1 Origen uses industry standard technologies to prevent unauthorized access or compromise of Origen's network, servers, or applications, which include such things as logical and physical controls to segment data, systems, and networks according to risk. Origen monitors demarcation points used to restrict access such as firewalls and security group enforcement points.

13.2 Users must authenticate with two-factor authentication prior to accessing Origen networks containing Customer Content.

14. Vendor Security

14.1 Origen conducts security due diligence and risk assessments of its vendors prior to onboarding and thereafter manages vendor security through its risk management program.

14.2 Origen management reviews the documented risks associated with vendors to understand the potential impact to the business. Mitigation plans are implemented to address material risks to business operations, including data protection.

14.3 Origen's agreements with vendors impose security obligations on them which are necessary for Origen to maintain its security posture as set forth in this Addendum. Confidential Information is shared only with those who are subject to appropriate confidentiality terms with Origen.

14.4 Origen uses a risk-based approach to monitor vendor security practices and compliance with their agreements with Origen.

15.1 15.2

16. Disaster Recovery Plan

16.1 Origen has a written Disaster Recovery Plan to manage significant disruptions to Origen Cloud SOLaaS operations and infrastructure. Origen management updates and approves the Plan annually.

16.2 Origen personnel perform annual disaster recovery tests. Test results are documented, and corrective actions are noted.

16.3 Data backup, replication, and recovery systems/technologies are deployed to support resilience and protection of Customer Content.

16.4 Backup systems are configured to encrypt backup media.

17. Asset Management and Disposal

17.1 Origen maintains and regularly updates an inventory of Origen Cloud SOLaaS ~~Platform~~ infrastructure assets and reconciles the asset list monthly.
17.2 Documented, standard build procedures are utilized for installation and maintenance of production servers.
17.3 Documented data disposal policies are in place to guide personnel on the procedure for disposal of Confidential Information, including Customer Content.
17.4 Upon expiration or termination of the Agreement, Origen will return or delete Customer Content in accordance with the terms of the Agreement. If deletion is required, Customer Content will be securely deleted, except that Customer Content stored electronically in Origen's backup or email systems may be deleted over time in accordance with Origen's records management practices.

18. Human Resources Security

18.1 Origen personnel sign confidentiality agreements and acknowledge Origen's Acceptable Use Policy during the new employee onboarding process.

19. CSA Proof of Compliance

19.1 19.2 19.2(I) PCI-DSS. Origen complies with the most recent version of PCI-DSS to the extent PCI-DSS is applicable to the Services provided under the Agreement (e.g., if Origen accesses, collects, uses, retains, discloses, processes, stores or transmits any Customer cardholder data as defined under PCI-DSS or any other data protected or subject to PCI-DSS), or if any part of such services impacts the security of the PCI Data environment.
19.2(ii) HIPAA. In the case of HIPAA (Health Insurance Portability and Accountability), Origen complies with the HIPAA security rule and data breach notification requirements for the processing of protected health information (PHI).