Commvault Security Terms

*These security terms set forth Commvault's technical and organisational measures as required by data privacy law. Any capitalized terms not defined herein shall have the meanings ascribed in the Master Terms and Conditions (the "**Agreement**").*

1. General Applicability.

1.1. **Scope.** These Security Terms ("**Security Terms**") apply to the Solutions and/or services provided under the Agreement, which may include Commvault's Software, SaaS Solution, and/or services.

1.2. **Precedence.** In the event of conflict between these Security Terms and the main body of the Agreement, these Security Terms shall prevail with respect to security-related matters, unless prohibited by applicable law.

2. Regulatory Compliance.

2.1. **Commvault Compliance.**

2.1.1 General. Commvault has implemented and maintains a security program designed to align with NIST 800-30/CSF and industry best practices. For its SaaS Solutions, Commvault maintains third-party certifications and assessments, including ISO 27001, SOC 2 Type II, HIPAA (including the processing of Protected Health Information), and PCI. For the up-to-date list of certifications, assessments, and additional attestations, please refer to our Trust Center: https://trust.commvault.com/resources.

2.1.2 FedRAMP. Our Government Cloud SaaS offering is FedRAMP High authorized and meets the FedRAMP High baseline control requirements based on NIST SP 800-53. For more information, see Commvault's FedRAMP Marketplace listing: https://marketplace.fedramp.gov/products/FR2115384377.

3. Shared Responsibility Model

3.1. **Data Use and Processing Limitations.** Commvault may use Customer Data solely for the purpose of delivering the Solutions in accordance with its Master Terms and Conditions and Data Processing Agreement. Commvault shall not process Customer Data for any other purpose without Customer's written consent.

3.2. **SaaS Solution Responsibilities.** Security and compliance for infrastructure and data protection operate under a shared-responsibility model. Commvault is responsible for securing the SaaS Solution and protecting Customer Data in transit and at rest within Commvault's Defined Service Boundary in accordance with the provisions set forth herein. "**Defined Service Boundary**" means the systems, infrastructure, and applications directly owned, operated, and controlled by Commvault for the delivery of the SaaS Solution, excluding without limitation Customer environments, Customer-managed configurations, identity providers, and any components outside Commvault's direct operational control. Customer is responsible for establishing and maintaining its own security and compliance programs as they relate to their use of the Commvault Solutions and/or services. This includes responsibility for security controls outside the Commvault's Defined Service Boundary, without limitation: (i) managing access to its applications and infrastructure, including authenticating users and managing credentials; (ii) maintaining appropriate endpoint protection; (iii) fulfilling all compliance obligations related to its data and environment; and (iv) lawful use of the Solutions. Our Documentation sets forth security and configuration guidance.

4. Security Posture & Monitoring

4.1. **Continuous Monitoring.** Commvault maintains continuous monitoring of the SaaS Solution in accordance with industry best practices, including without limitation, vulnerability scanning, threat detection, configuration compliance checks, and logging of security events.

4.2. **DevSecOps & Testing.** Commvault embeds security reviews within its development lifecycle, including secure code reviews, static/dynamic analysis, and annual penetration tests.

4.3. **Remediation.** Commvault maintains processes to identify and remediate vulnerabilities in accordance with its internal policies. For the SaaS Solution, Commvault shall use commercially reasonable efforts to remediate critical vulnerabilities within 30 days and high-severity vulnerabilities within 60 days, unless otherwise agreed in writing with Customer.

5. Security Compliance

5.1. **Access Control.** Commvault's personnel and systems are subject to access management controls designed to protect Customer Data from unauthorized access in accordance with Section 4.2 (Access) of the SaaS Solution Terms and Conditions. Such controls include, where applicable, multi-factor-authentication, least privilege and role-based access, segregation of duties, access approval procedures, regular access reviews, and procedures to revoke stale access.

5.2. **Awareness and Training.** Commvault maintains an annual training and awareness program which aligns with applicable law and is independently verified by external auditors to monitor effectiveness and integrity.

5.3. **Audit Rights**

5.3.1. Independent Audits. Validation of compliance is evidenced through documentation including but not limited to third-party audit reports available at: https://trust.commvault.com/resources.

5.3.2. Customer Audit Rights.

5.3.2.1 Upon request, Commvault will make available current security and compliance documentation, including third-party audit reports, certifications, penetration test summaries, security whitepapers, and control descriptions ("**Security Documentation**").

5.3.2.2 Customer may exercise audit rights by submitting a reasonable, written security or compliance questionnaire no more than once annually or following a material security incident affecting Customer Data. Commvault will respond in good faith, within a commercially reasonable timeframe, either by completing the questionnaire or providing substantively equivalent information.

5.3.2.3 Customer acknowledges that audit rights exclude on-site inspections, facility or system access, personnel interviews, access to infrastructure, source code, logs, internal records, evidentiary artifacts (including screenshots or configurations), and any technical testing (including penetration tests, vulnerability scans, or social-engineering exercises).

5.4. **Contingency Planning.** Commvault maintains a business continuity and disaster recovery plan for the SaaS Solution, which is subject to periodic testing. The SaaS Solution infrastructure is designed to support global redundancy, rapid failover capabilities, and disaster recovery isolation. Commvault's business continuity and disaster recovery plan is validated annually by its third-party auditors.

5.5. **Configuration Management.** For the SaaS Solution, all systems supporting Customer Data follow secure configuration baselines, and changes are controlled through documented workflows that include testing and authorization procedures. Configuration changes are tracked and monitored while access to configuration changes is restricted to authorized personnel.

5.6. **Identification and Authentication.** Commvault shall make available authentication controls for Customer's Authorized Users accessing the Solutions and/or services, including multi-factor authentication (MFA),

single sign-on (SSO) via SAML or OAuth, and integration with Customer's identity providers.

5.7. **Incident Response**

5.7.1. **Procedures.** Commvault maintains documented incident response procedures, including defined roles, escalation paths, and communication protocols.

5.7.2. Unless otherwise required by law, Commvault agrees to notify Customer of any Security Breach within seventy-two (72) hours following Commvault's confirmation thereof. Customer shall cooperate with Commvault's incident response procedures as required.

5.7.3. "**Security Breach**" means an accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to unencrypted Customer Data.

5.7.4. **Contact Information.** Customer may report a Security Breach or concerns to Commvault's Security Incident Response Team at soc@commvault.com.

5.7.5. **Investigation and Forensics.** For any Security Breach requiring investigation, Commvault shall: (i) conduct appropriate digital forensic analysis using industry-standard tools and methodologies; (ii) preserve relevant evidence in accordance with applicable law; (iii) perform root cause analysis to determine the source and scope of the incident; and (iv) implement corrective measures to prevent recurrence, subject to reasonable business considerations and system limitations. In accordance with this Section 5.7.5, Commvault may provide Customer with a summarized report upon request.

5.7.6. **Third-Party Coordination.** For Software: Customer shall lead incident response activities and coordinate with appropriate third parties as Customer deems necessary. Commvault shall provide reasonable support and assistance to Customer in connection with such incident response activities. For the SaaS Solution: Where legally required or operationally necessary, Commvault may coordinate incident response activities with appropriate third parties, including law enforcement agencies, regulatory authorities, cloud infrastructure providers, and other security vendors. In both cases, the coordinating party shall notify the other party of such coordination when legally permissible and operationally feasible, provided that Customer's confidential information shall be protected to the extent possible under the circumstances.

5.8. **Maintenance.** Commvault shall monitor the SaaS Solution's availability and perform testing of infrastructure availability. Commvault periodically releases patches, fixes, upgrades, updates or new versions (together, the "Updates") Customers using our Software are responsible for maintaining and implementing Updates to the Software.

5.9. **Media Protection.** For the SaaS Solution, Commvault utilizes reputable third-party cloud infrastructure providers that maintain media protection controls aligned with their published security standards. Media sanitization and destruction processes for Customer Data are performed in accordance with the standards and procedures of the applicable third-party cloud service providers. For Software, Customer is solely responsible for implementing media protection measures, including the sanitization and destruction of any media containing Customer Data within Customer's environment.

5.10. **Physical and Environmental Protection.** Customer Data is protected by physical controls, including but not limited to secured facilities and equipment, authorized and documented personnel access, restricted server areas, monitored and logged facility access, and supporting security and authentication systems.

5.11. **Program Management.** Commvault maintains an information security program that includes: (a) a defined organizational structure, and documented policies, roles, responsibilities, and strategic objectives; (b) risk management through periodic risk assessments, and formal processes to identify, assess, mitigate, and track security risks; (c) a security controls framework aligned with industry standards; (d) security testing to address potential attack vectors and a multi-layered security approach in development and operations; (e) training and development programs for security personnel; and (f) periodic review and updates of the program.

5.12. **Personnel Security.** Except as prohibited by law, Commvault shall conduct background checks for employees with access to Customer Data in accordance with applicable law. Commvault maintains an onboarding process for confidentiality obligations and policy acknowledgments, employment policies, processes for role changes and terminations.

5.13. **Risk Assessment.** Commvault maintains security policies designed to support alignment with applicable security standards, security testing and vulnerability identification processes which may include penetration testing and vulnerability disclosure programs, vulnerability management processes, and security evaluations, all conducted in accordance with its internal policies. Evidence of independent audits is available as referenced in Section 5.3.1.

5.14. **System and Information Integrity**

5.14.1. **Encryption.** Commvault shall encrypt Customer Data in transit using current versions of TLS or other security protocols with strong encryption algorithms, and at rest using current versions of AES encryption algorithms in accordance with industry standards.

5.14.2. **Key Management.** Encryption keys are stored securely in an encrypted database protected by role-based access control and optionally a passphrase. Integration with external Key Management Services (as define below) is supported for enhanced security and separation in accordance with section 5.14.3.

5.14.3. **Third-Party Key Management Services.** If technically feasible and Customer elects to use a third-party Key Management Service ("**KMS**"), Customer shall be solely responsible for securing such KMS by taking, at a minimum, the following measures: (i) implementing NIST 800-57 or equivalent industry standard security controls to protect the KMS; and (ii) backing up the encryption keys to a virtually air-gapped environment. Commvault expressly disclaims any and all liability related to, or arising from, the Customer's use of the third-party KMS, including inability to access data resulting from such use. Commvault is not responsible or liable for the manner in which the third-party KMS transmits, accesses, processes, stores, uses or provides data to Commvault.

5.15 **Supply Chain Risk Management.** Commvault shall conduct risk-based assessments of suppliers, maintain records of suppliers, conduct periodic reviews of supplier documentation and assessments, and implement security measures for third-party access.

5.16 **Data Integrity and Quality Controls.** Within Commvault's Defined Service Boundary, Commvault maintains controls designed to support data integrity and quality, which may include: (a) authorization policies for input, reading, alteration, and deletion of data; (b) authentication of authorized personnel; (c) protective measures for data operations including logging of material changes where appropriate; (d) segregation and protection of data via database schemas, logical access controls, and/or encryption; (e) utilization of user identification credentials; and (f) session management controls. These controls are maintained in accordance with Commvault's internal security policies.

6. **Data Localization.** Commvault shall store and process Customer Data in the geographic regions specified in the applicable Documentation, with options for regional data residency as set forth therein.

7. **Change Management**

7.1. **Notice of Changes.** Commvault shall provide at least 30 days' prior written notice of material changes to its security policies or controls that

may adversely affect Customer Data.

7.2. **Termination.** If such change materially degrades security, Customer may terminate the affected Solutions and/or services without penalty, provided however that all sales of Software are final, non-returnable and non-refundable.

8. Cloud Provider Commitments. Commvault leverages third-party cloud infrastructure providers, which may include Microsoft Azure, AWS, GCP, and/or Oracle Cloud Infrastructure, for SaaS Solution provisioning. Commvault inherits certain security measures from these cloud providers. Security documentation for each cloud provider is available at their respective trust centers.

9. Applicable Jurisdictions & Sub-Modules

9.1. **Global Framework.** These Security Terms are intended for global use and shall apply except as overridden by mandatory local law.

9.2. **Regional and Sectoral Annexes.** Regional and Sector-Specific annexes (e.g., Commvault Customer Data Agreement, HIPAA Addendum, Financial Sector Addendum) shall supplement and, where required, override these Security Terms solely to the extent necessary for compliance.

CUSTOMER	**COMMVAULT**
Name:	**Name:**
Date:	**Date:**