Vulnerability Disclosure Policy

PURPOSE

This Vulnerability Disclosure Policy (the "Policy") outlines the commitment of Commvault Systems, Inc. and its affiliates ("Commvault") to maintaining the security and integrity of its products, systems, and data. The purpose of this Policy is to provide clear framework for security researchers and other stakeholders to report Vulnerabilities responsibly, and to outline Commvault's process for acknowledging, investigating, and remediating such reports.

SCOPE

This Policy applies to:

- All Commvault's Solutions (including products, Software, SaaS), services and systems.
- All individuals or entities conducting or submitting security research involving Commvault's digital assets.

Any vulnerability that affects the integrity of Commvault's solutions or the confidentiality of the information stored within will be in scope for this program.

DEFINITIONS

Vulnerability. A flaw or weakness in a system, software, or process that could be exploited to compromise security.

Security Researcher. Any individual or entity who investigates, tests, or discloses security vulnerabilities.

Personally Identifiable Information ("PII"). Any data that can be used to identify an individual (e.g., names, IDs, email addresses).

Denial-of-Service ("DoS") Attack. An attempt to make a system or network resource unavailable to its users.

POLICY

Commvault requires all security research on its products, software, and systems to adhere to the following principles:

Act in good faith. Conduct all Vulnerability research in an ethical and legal manner with the intent to improve security.

Use authorized testing. Only perform testing on systems or accounts that you own or are explicitly permitted to test.

Stop testing and report immediately. If you encounter any sensitive data, such as PII, financial information, information marked as confidential or trade secrets, stop your testing and report the issue immediately. Do not store, share, or further process this data.

Do not:

- Disclose any unpublished Vulnerability or its details to a third party without written consent from Commvault.
- Access, modify, or delete data you do not own.

- Disrupt Commvault's Solutions or systems.
- Use DoS attacks.
- Attack Commvault facilities or personnel.
- Social engineer Commvault employees.
- Exploit the Vulnerability beyond the minimal testing required to prove its existence.
- Violate any laws, regulations or Commvault product terms to identify vulnerabilities.

Reporting a potential vulnerability. All Vulnerability reports should be submitted to via email at PSIRT@Commvault.com. By reporting a Vulnerability to Commvault, you acknowledge and agree to this Policy. Please include the following information about the Vulnerability in the report:

- A detailed description.
- Steps to reproduce.
- Potential impact as per your assessment
- Affected systems/URLs.
- Contact information, with email address

Commvault's Commitment. Upon receiving a Vulnerability report in accordance with this policy, Commvault will:

- Acknowledge receipt of your report within 2 business days.
- Investigate and take reasonable steps to validate the report.
- Maintain communication and provide updates on the investigation, timelines and remediation.
- Remediate the Vulnerability as appropriate within a reasonable timeframe.

Public Disclosure. Commvault reserves the right to determine the scope, timing, and method of public disclosure for Vulnerabilities affecting its Solutions, services and systems in accordance with coordinated vulnerability disclosure best practices and with due consideration for customer security and operational impact, and you agree to refrain from disclosing any Vulnerability without coordinating the disclosure with Commvault. We will make all efforts to remediate all valid vulnerabilities in a reasonable time. Commvault will endeavor to publish CVEs for all valid Vulnerabilities in scope, that are CVSS 7.0 (high) or greater, within 2 weeks of a fix becoming available.

Recognition. We appreciate the efforts of security researchers who help us improve our security. We may offer recognition for valid Vulnerability reports in our sole discretion. If anonymity is preferred, please note such preference in the Vulnerability report.

ADMINISTRATION

Ownership. This Policy is owned by Corporate Trust and reviewed at least annually. The Company reserves the right to change this Policy at any time and publish the current version to Commvault's website. General inquiries regarding use of this Policy may be directed to PSIRT@Commvault.com. Exceptions to this Policy must be approved by the Company's Chief Trust Officer.

Reporting & Enforcement. Individuals may report potential or actual violations of this Policy to compliance@commvault.com. Confidential and anonymous reporting is available through the Company's Ethics and Integrity Reporting Platform by visiting https://integritycounts.ca/org/commvault or emailing on commvault@integritycounts.cawh. The Company prohibits retaliation against any individual who makes a good faith report. Violations of this Policy may result in disciplinary action, up to and including termination of employment or contractual relationship.

Policy Updates

Commvault reserves the right to modify this policy at any time. We encourage review of this policy periodically for any changes.