mimecast

Code42 Incydr Services TOMs

Last Updated August 2024

This document describes technical and organizational security measures and controls implemented to protect the data Customers entrust to us as part of the Incydr Service. Mimecast acquired Code42 in July 2024.

Within this document, the following definitions apply:

- "Customer" means any subscriber to the Incydr Service.
- "Incydr Services" means the Incydr Service provided to our Customers.
- "Customer Data" means any information provided or submitted by the Customer that is processed by the Incydr Service.
- "Personal Data" means any information relating to an identified or identifiable natural person.
- "Personnel" means Code42 employees and authorized individual contractors/vendors.
- "Strong Encryption" means the use of industry standard encryption measures.

Mimecast may change these measures from time to time to adapt to the evolving security landscape and where required will notify customers of material changes.

1. Purpose

a. This describes the minimum information security standards that Code42 maintains to protect your Customer Data processed through the Incydr Service.
b. Code42 follows AICPA guidelines and regularly reviews controls as described in Code42's SOC2 Type II independent auditor report ("SOC2 Report").

2. Encryption and key management

a. Code42 uses industry-standard encryption techniques to encrypt Customer Data at rest and in transit.
b. All connections are authenticated and encrypted using industry standard encryption technology.
c. Code42's key generation utilizes keys that are generated with methods consistent with industry accepted best practices and is reviewed on an annual basis.
d. Customer Data is checked for integrity during transit to provide Code42 the ability to detect data tampering or corruption.

3. Support and maintenance

Code42 deploys changes to the Cloud Services during scheduled maintenance windows, details of which are posted to the Code42 website prior to the scheduled period. In the event of a service interruption, Code42 posts a notification to the website describing the affected services. Code42 provides status updates, high level information regarding upgrades, new release availability, and minimum release version requirements via the Code42 website

4. Incident response and notification

a. "**Incident**" means a security event that compromises the confidentiality, integrity or availability of a Code42 information asset. "**Breach**" means an Incident that results in the confirmed disclosure, not just potential exposure, of Customer Data to an unauthorized party.
b. Code42 has an incident response plan, including a breach notification process, to assess, escalate, and respond to identified physical and cyber security Incidents that impact the organization, customers, or result in data loss. Discovered intrusions and vulnerabilities are resolved in accordance with established procedures. The incident response plan is reviewed and updated annually and more frequently as needed.
c. If there is a Breach involving your Customer Data, Code42 will (A) notify you within 24 hours of discovery of the Breach, (B) reasonably cooperate with you with respect to such Breach, and (C) take appropriate corrective action to mitigate any risks or damages involved with the Breach to protect your

Customer Data from further compromise. Code42 will take any other actions that may be required by applicable law as a result of the Breach.

5. Code42 security program

a. **Scope and Contents.** Code42 maintains a written security program that (A) complies with applicable global industry recognized information security frameworks, (B) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data and (C) is appropriate to the nature, size and complexity of Code42's business operations.

b. **Security Program Changes.** Code42 policies (including the Code42 Code of Conduct), standards, and operating procedures related to security, confidentiality, integrity and availability are made available to all Code42 Personnel via the corporate intranet. Security policies are reviewed, updated (as needed), and approved at least annually to maintain their continuing relevance and accuracy. Code42 Personnel are required to review and acknowledge Security policies during on-boarding and annually thereafter.

c. **Security Officer.** The Code42 Chief Information Security Officer and security team develop, maintain, review and approve Code42 Security Policies.

d. **Security Training & Awareness.** All Code42 Personnel are required to complete security awareness training at least annually. Code42 conducts periodic security awareness education to give Code42 Personnel direction for creating and maintaining a secure workplace.

6. Risk management

a. Code42 has a security risk assessment and management process to identify and remediate potential threats to Code42. Risk ratings are assigned to all identified risks, and remediation is managed by security Personnel. Executive management is kept apprised of the risk posture of the organization.

b. Code42 has an established insider threat risk management program to monitor, alert and investigate threats posed by both non-malicious and malicious actors inside the organization on an on-going basis. Identified issues are reviewed and investigated as appropriate.

c. **Threat and vulnerability management and security testing.** Code42's Threat and Vulnerability Management (TVM) program monitors for

vulnerabilities on an on-going basis. Code42 conducts monthly internal and external vulnerability scans using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated, documented, and remediated to address the associated risk(s). Ongoing bug bounty and external penetration tests are conducted annually by an independent third party. Findings from these tests are evaluated, documented, and remediated.

7. Access management

a. Code42 assigns application and data rights based on security groups and roles, which are created based on the principle of least privilege. Security access requests are approved by the designated individual prior to provisioning access.
b. Code42 classifies informational assets in accordance with the Code42 data classification guideline.
c. Access to Code42 systems and networks is disabled promptly upon notification of termination.
d. Code42 reviews administrator access to confidential and restricted systems, including corporate and cloud networks, on a semiannual basis. Code42 reviews administrator access to the cloud production environment and to select corporate systems that provide broad privileged access on a quarterly basis. Any inappropriate access is removed promptly.
e. Code42 uses separate administrative accounts to perform privileged functions, and accounts are restricted to authorized Personnel.

8. Password management and authentication controls

Authentication mechanisms require users to identify and authenticate to the corporate network with their unique user ID and password. Code42 requires minimum password parameters for the corporate network via a directory service system.

9. Remote access and cloud access

Remote access to the corporate network is secured through a virtual private network (VPN) solution with two-factor authentication. Access to the cloud network requires two authentication steps; authorized users must log on to the

corporate network and then authenticate using separate credentials through a jump box server.

10. Asset configuration and security

Endpoint detection and response (EDR) technology is installed and activated on all Code42 endpoints to monitor for virus and malware infections. Endpoint devices are scanned in real-time. Monitoring is in place to indicate when an anti-virus agent does not check in for prolonged periods of time. Issues are investigated and remediated as appropriate. Virus definition updates are automatically pushed out to endpoint devices from the EDR technology as they become available. Code42 uses full-disk encryption on endpoint devices. Endpoint devices are monitored and encrypted using industry recognized tools. Code42 has tools to identify and alert IT administrators of discrepancies between Code42 security policies and a user's endpoint settings. Code42 maintains and regularly updates an inventory of corporate and cloud infrastructure assets, and systematically reconciles the asset inventory annually.

11. Logging and Monitoring

Code42 continuously monitors application, infrastructure, network, data storage space and system performance. Code42 utilizes a security information event monitoring (SIEM) system. The SIEM pulls real-time security log information from servers, firewalls, routers, intrusion detection system (IDS) devices, end users and administrator activity. The SIEM is configured for alerts and is monitored on an ongoing basis. Logs contain details on the date, time, source, and type of events. Code42 reviews this information and works events worthy of real-time review.

12. Change management

Code42 has change management policies and procedures for requesting, testing and approving application, infrastructure and product related changes. All changes receive a risk score based on risk and impact criteria. Low risk changes generate automated change tickets and have various levels of approval based on risk score. High risk changes require manual change tickets to be created and are reviewed by approvers based on change type. Planned changes to the corporate or cloud production environments are reviewed regularly. Change

documentation and approvals are maintained in a ticketing system. Product development changes undergo various levels of review and testing based on change type, including security and code reviews, regression, and user acceptance testing prior to approval for deployment. Following the successful completion of testing, changes are reviewed and approved by appropriate managers prior to implementation to production. Code42 uses dedicated environments separate from production for development and testing activities. Access to move code into production is limited and restricted to authorized personnel.

13. Secure development

Code42 has a software development life cycle (SDLC) process, consistent with Code42 security policies, that governs the acquisition, development, implementation, configuration, maintenance, modification, and management of Code42 infrastructure and software components. Prior to the final release of a new Code42 system version to the production cloud environment, code is pushed through lower tier environments for testing and certification. Code42 follows secure coding guidelines based on leading industry standards. These guidelines are updated as needed and available to personnel via the corporate intranet. Code42 developers receive annual secure coding training. Code42 utilizes a code versioning control system to maintain the integrity and security of the application source code.

14. Network security

Code42 uses network perimeter defense solutions, including an IDS and firewalls, to monitor, detect and prevent malicious network activity. Security personnel monitor items detected and take appropriate action. Firewall rule changes (that meet the criteria for the corporate change management criteria) follow the change management process and require approval by the appropriate approvers. Code42's corporate and cloud networks are logically segmented by virtual local area networks (VLANs) and firewalls monitor traffic to restrict access to authorized users, systems and services.

15. Third party security

Code42 assesses and manages the risks associated with existing and new third party vendors. Code42 employs a risk-based scoring model for each third party. Code42 requires third parties to enter into contractual commitments that contain security, availability, processing integrity and confidentiality requirements and operational responsibilities as necessary. Code42 evaluates the physical security controls and assurance reports for data centers on an annual basis. Code42 assesses the impact of any issues identified and tracks any remediation efforts.

16. Physical security

Code42 grants access to data centers and Code42 offices by job responsibility, and access is removed as part of the Code42 separation or internal job transfer process when access is no longer required. Access to Code42 offices is managed by a badging system that logs access, and any unauthorized attempts are logged and denied. Code42 personnel and visitors are required to display identity badges at all times within Code42 offices. Code42 maintains visitor logs and requires visitors to be escorted by Code42 personnel.

17. Oversight and audit

Internal audits are aligned to Code42's information security program and compliance requirements. Code42 conducts internal control assessments to validate that controls are operating effectively. Issues identified from assessments are documented, tracked and remediated. Internal controls related to security, availability, processing integrity and confidentiality are audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards.

18. Business continuity plan

Code42 maintains a Business Continuity Plan and a Disaster Recovery Plan to manage significant disruptions to Code42 operations and infrastructure. These plans are reviewed and updated periodically and approved on an annual basis. Code42 conducts business continuity exercises to evaluate Code42 tools, processes and subject matter expertise in response to specific incidents. Results

of these exercises are documented and any issues identified are tracked to remediation.

19. Human resources security

Code42 has procedures in place to guide the hiring process. Background verification checks are completed for Code42 Personnel in accordance with relevant laws and regulations. Code42 requires Personnel to sign a confidentiality agreement as a condition of employment. Code42 maintains a disciplinary process to take action against Personnel that do not comply with company policies, including Code42 security policies.