Information security addendum

Effective May 14, 2019

This Information Security Addendum ("Addendum") applies whenever it is incorporated by reference into the Master Services Agreement ("Agreement"). Capitalized terms used but not defined in this Addendum have the meanings ascribed in the Agreement.

1. Purpose

1.1 This Information Security Addendum describes the minimum information security standards that Code42 maintains to protect your Customer Data. Requirements in this Addendum are in addition to any requirements in the Agreement.

1.2 For the Enterprise, Premium and Classic product offerings (collectively "enterprise offerings"), Code42 follows AICPA guidelines and regularly reviews controls as described in Code42’s SOC2 audit report. For your convenience, Code42 references some of the applicable SOC2 controls in this Addendum. Code42 will provide you with a copy of the SOC2 independent auditor report upon request.

1.3 The CrashPlan for Small Business offering is not currently SOC2 certified, and the cross-references to specific SOC2 controls (e.g. SOC: A-4) are not applicable.

2. Data storage

You decide if Customer Data is backed up to your data centers, Code42 data centers, or both.

3. Encryption and key management

3.1 You have the ability to disable encryption in some Code42 products, and if you do then the sections of this Addendum relating to encryption do not apply to your Customer Data.

3.2 Code42 uses industry-standard encryption techniques to encrypt Customer Data at rest and in transit (SOC: A-4, SOC: C-10). The Code42 System is configured by default to encrypt user data files at the source using AES 256-bit encryption. Customer data remains encrypted in transit and at rest, and decryption is controlled by the customer (SOC: C-8). Code42 encrypts and secures your encryption keys within the authority server and securely transfers those keys during the sign-in process (SOC: C-11). Code42 has a policy and process for managing encryption keys for file data blocks, which includes security requirements for key creation, use, storage, and protection. Code42 generates encryption keys using a secure random number generated based on a global industry recognized information security framework (SOC: C-12).
3.3 Code42 uses industry standard encryption technologies for data contained within, accessed by, or transmitted through Code42 systems in accordance with data classification standards (SOC: C-10). Once files are encrypted and secured at the source, the Software sends backup transmissions to the destination server(s) using the 256-bit AES Transport Layer Security (TLS) encryption protocol (SOC: LA-19). Transmitted Customer Data is MD5 check-summed at multiple points during the backup process, including after encryption at the source to provide destinations the ability to detect tampering without having encryption keys for the original data (SOC: C-9).

4. 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. If additional maintenance is needed, Code42 notifies impacted customers in advance of scheduled maintenance occurring outside of the scheduled window (SOC: CM-11). Code42 communicates upgrades, new releases, and minimum release version requirements to customers via the Code42 support website (SOC: CM-12).

5. Incident response and notification

5.1 "Incident" means a security event that compromises the integrity, confidentiality or availability of an information asset. Code42 has an incident response plan and team to assess, escalate, and respond to identified physical and cyber security Incidents that impact the organization or customers or result in data loss. Code42 reviews and updates this plan annually and as needed throughout the year. The incident response team resolves intrusions and vulnerabilities upon discovery and in accordance with the established procedures.

5.2 "Breach" means an Incident that results in the confirmed disclosure, not just potential exposure, of data to an unauthorized party. If Code42 determines that an Incident has led to a Breach, Code42 will follow its breach notification process (SOC: OPS-5). Incident management and escalation procedures exist to ensure that Code42 addresses system issues, problems and security-related events, in a timely manner, and that all Incidents are logged, prioritized, and resolved based on established criteria and severity levels (SOC: OPS-4).

5.3 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 any 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.

6. Code42 security program

6.1 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 data and (C) is appropriate to the nature, size and complexity of Code42’s business operations.
6.2 Security Program Changes. Code42 has policies, standards, and operating procedures related to security, availability and confidentiality that are available to personnel via the corporate intranet. Code42 reviews, updates and approves security policies and procedures at least annually to maintain their continuing relevancy and accuracy. Personnel acknowledge security policies during onboarding and annually thereafter (SOC: ORG-3). The Code42 Privacy Policy describes confidentiality and privacy commitments to our customers and is posted on the Code42 website (SOC: C-3).

6.3 Security Officer. The Code42 Chief Security Officer and Governance, Risk and Compliance group develop, maintain, review, and approve Code42’s security, availability, and confidentiality standards and policies (SOC: ORG-4).

6.4 Security Training & Awareness. Code42 personnel complete security awareness training on an annual basis, and re-acknowledge the Code of Conduct and other Code42 policies as appropriate (SOC: ORG-11). Code42 conducts periodic security awareness campaigns to educate personnel about their responsibilities and give them direction for creating and helping to maintain a secure workplace (SOC: COM-11).

7. Risk management

Code42 has a formal security risk assessment and management process to identify potential threats to the organization. Code42 management rates and reviews all identified risks (SOC: RM-2).

8. Access control program

8.1 Code42 manages access to internal and external applications via Active Directory user security groups. Code42 allocates System privileges and permissions to users or groups on a least privilege principle (SOC: LA.1). Code42 assigns application and data rights based on user groups and roles, and grants access to information based on job function (SOC: C-5).

8.2 Code42 allocates system privileges and permissions to users or groups on a least privilege principle. Code42 classifies informational assets in accordance with the Code42 data classification requirements.

9. User access management

Code42 requires approved access requests prior to granting new user access and changing existing user access to the corporate and cloud networks and systems (SOC: LA-7). Code42 promptly disables application, platform and network access for terminated users upon notification of termination (SOC: LA-8). Code42 reviews access privileges to internal systems and the corporate and cloud networks, including administrative access privileges, on a quarterly basis (SOC: LA-9). Code42 uses separate administrative accounts to perform privileged functions and are restricted to authorized individuals (SOC: LA-10).
10. Password management and authentication controls

Authorized users must identify and authenticate to the network, applications, and platforms using their unique user ID and password. The Active Directory system requires Minimum password parameters for access to the Corporate network (SOC: LA.2).

11. Remote access and cloud access

A Virtual Private Network (VPN) solution with two-factor authentication secures remote access to the corporate network (SOC: LA-3). 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 secure shell (SSH) jump box server (SOC: LA-4).

12. Asset configuration and security

All Code42 workstations have active anti-virus (AV) software installed to monitor for virus and malware infections. Endpoint devices are scanned in real-time and a full system scan is performed weekly. Monitoring is in place to indicate when an anti-virus agent does not check in for prolonged periods of time. The Security Operations Team investigates and takes action to resolve issues as appropriate. Virus definition updates are pushed out to endpoint devices automatically from the AV software central administration console as they become available (SOC: LA-12). Code42 uses full-disk encryption on Code42 endpoints. End-point configuration is managed using JAMF Software Server (JSS) and System Center Configuration Manager (SCCM) tools and IT administrators are alerted of discrepancies in security policies and settings identified from the tools (SOC: LA-13). Code42 maintains and regularly updates an inventory of corporate and Cloud infrastructure assets, and systematically reconciles the asset list annually (SOC: OPS-6).

13. Threat and vulnerability management and security testing

Code42 has a Threat and Vulnerability Management (TVM) program to monitor for vulnerabilities on an on-going basis that are acknowledged by vendors, reported by researchers, or discovered internally through vulnerability scans, Red Team activities, and personnel identification. Code42 documents vulnerabilities within a security risk ticket and ranked based on severity, which is determined by the likelihood and impact ratings assigned. Code42 assigns tickets to the appropriate team(s) for remediation and vulnerabilities are tracked to resolution (SOC: RM-3). Weekly internal and external vulnerability scans are conducted using an industry-recognized vulnerability scanning tool. Code42 evaluates and documents identified vulnerabilities within a security risk ticket, and remediates to address the associated risks (SOC: RM-6). For enterprise offerings only, an external vendor conducts security penetration tests on the corporate and cloud environments at least annually to detect network and application security vulnerabilities. Critical findings from these tests are evaluated, documented within a risk ticket and assigned to the Product Security team for remediation (SOC: RM-7).
14. Logging and monitoring

Code42 continuously monitors application, infrastructure, network, data storage space and system performance (SOC: OPS-1). A monitoring system pulls security log information from servers, firewalls, routers, and Intrusion Detection System devices on a real-time basis. Logs contain details on the date, time, source, and type of events. The Security Operations Team reviews key reports daily and follows up on events, as necessary (SOC: OPS-2). System logging is enabled for end user and administrator activity and is reviewed as necessary, including failed and successful login attempts and updates executed by privileged Code42 system users (SOC: OPS-3).

15. Change management

Code42 follows documented change management policies and procedures for requesting, testing, and approving application, infrastructure, and product related changes (SOC: CM-1). Changes undergo various levels of review and testing, including security and code reviews, regression, and user acceptance prior to approval for implementation (SOC: CM-2). Following the successful completion of testing, the appropriate managers must approve changes prior to implementation in a production environment (SOC: CM-3). Dedicated environments separate from production exist for development and testing activities. Logical access controls requiring two-factor authentication secure these separate environments. Only authorized individuals can move code into production (SOC: CM-10).

16. Secure development

Code42’s Software Development Life Cycle (SDLC) methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components. The SDLC methodology is consistent with the defined Code42 security, availability, and confidentiality policies (SOC: CM-5). Developers use secure coding guidelines based on leading industry standards, and receive annual secure coding training (SOC: CM-8). For each product release, Code42 performs a security architecture review and conducts a vulnerability scan and static code analysis in the development environment. Identified vulnerabilities and coding defects are resolved prior to implementation (SOC: CM-6). Prior to final release of a new Code42 version to the production Cloud environment, an internal rollout is performed within the Code42 internal cloud to test and troubleshoot the product (SOC: CM-7). Code42 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 (SOC: CM-9).

17. Network security

Network perimeter defense solutions, including an Intrusion Detection System (IDS) and firewalls, are in place to monitor, detect, and prevent malicious network activity. Security operations personnel monitor items detected and take appropriate action (SOC: LA-16). Firewall configurations and rules are reviewed at least annually. Significant changes to firewall rules follow the Change Management process and require approval by the Change Advisory Board (SOC: LA-17). 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 (SOC: LA-18).
18. Third party security

Code42’s vendor management team assesses the risk associated with new vendors prior to onboarding, and has an ongoing risk management process for existing vendors. The vendor management team employs a risk based vendor scoring model that accounts for data access, network connectivity, compliance impacts and sub-vendor usage among other elements (SOC: MON-3). Code42 communicates security and confidentiality requirements and operational responsibilities to third parties through contractual agreements (SOC: COM-9). Code42 evaluates physical security controls at each co-location data center on a quarterly basis. This includes reviewing the applicable security assurance reports (e.g. SOC 1/2 and ISO 27001) and contractual obligations. The impact of any issues identified is assessed and, if necessary, remediation is tracked by the Security Team. Code42 conducts onsite reviews of contracted data centers on an as-needed basis (SOC: MON-4).

19. Physical security

Code42 grants physical access to Code42 facilities (including data centers where standing-access is necessary for certain employees) based on job responsibilities. Code42 removes physical access when access is no longer required and as a component of the employee termination process (SOC: LA-23, SOC: LA-26). Personnel and visitors must display identity badges at all times within Code42 facilities. Code42 maintains visitor logs and escorts visitors at all times (SOC: LA-24). Badge readers control access to restricted areas within Code42 office facilities and data center locations. Unauthorized badge access attempts are denied and logged. Tailgating is prohibited by Code42 policy (SOC: LA-22). For data centers that do not require standing-access, access is granted only for the duration of a data center visit based on an approved access request. Access to data center facilities can only be approved by the Physical Security department (SOC: LA-25). Code42 reviews data center physical access, including remote access, on a quarterly basis to confirm that access is restricted to authorized personnel.

20. Oversight and audit

Code42 conducts internal control assessments on a quarterly basis to validate that controls are designed and operating effectively. Issues identified from assessments are documented, tracked and remediated as appropriate. (SOC: MON-1). For enterprise offerings only, internal controls related to security, availability, and confidentiality are audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards. Code42 documents and tracks the resulting auditor findings for remediation. Independent audit reports are available to potential and current customers upon request (SOC: MON-2).

21. Business continuity plan

Code42 has a Business Continuity Plan and a Disaster Recovery Plan in place to manage significant disruptions to Code42 operations and infrastructure. Code42’s Chief Security Officer reviews, updates and approves these plans annually (SOC: A-5). Code42 conducts exercises to evaluate the tools, processes and subject matter expertise of Code42 in response to a specific incident. Code42 documents a summary of the exercise results, and any tracks and remediates any issues identified (SOC: A-6).
22. Human resources security

Code42 personnel sign a confidentiality agreement and acknowledge security policies during the new employee on-boarding process (SOC: C-2). Code42 conducts background verification checks for potential Code42 personnel in accordance with relevant laws and regulations. The background checks are commensurate to an individual’s job duties and include at a minimum social security verification and a criminal history check (SOC: ORG-8). Code42 maintains a disciplinary process to take action against personnel that do not comply with company policies, including but not limited to, those put in place to meet its security, availability and confidentiality commitments and requirements (SOC: ORG-5).