

Exhibit A

Service level agreement

Effective July 15, 2020

This Code42 Service Level Agreement (“SLA”) applies whenever it is incorporated by reference into the Master Services Agreement (“Agreement”) between you and Code42. This SLA does not apply to the CrashPlan for Small Business offering. Capitalized terms used but not defined in this SLA have the meanings given to them in the Agreement.

1. Service commitment

Code42 will provide the Code42 Offering with at least 99.9% Availability during each calendar month. If Code42 does not meet this commitment, you are eligible to receive a Service Credit as described below.

2. Definitions

2.1 “Availability” means you are able to (A) perform searches of indexed file events, and (B) retrieve files collected and preserved by Code42.

2.2 “Cloud Storage” means Code42’s cloud-based storage service for files from endpoint devices.

2.3 “Code42 Offering” means Code42’s Cloud Storage and/or Security Event Service.

2.4 “Security Event Service” means Code42’s cloud-based security service for indexing and searching file activity.

2.5 “Service Credit” means a dollar credit, calculated as described below, that Code42 credits back to an eligible Code42 account.

2.6 “Monthly Uptime Percentage” means for any calendar month a percentage calculated as follows:

$$\frac{\text{Total minutes available for all users}}{(\text{Total minutes in month} - \text{Scheduled maintenance}) \times \text{Number of users}}$$

3. Service credits

Service Credits are a percentage of the fee paid to Code42 for the Code42 offering during the calendar month in which Code42 did not meet the Availability commitment. If you paid an annual fee or purchased the Code42 Offering as part of a suite or bundle of products, Code42 will calculate Service Credits based on the pro rata portion of the total fee attributable to the Code42 Offering for the applicable month. Service Credit percentages are as follows:

Monthly uptime percentage	Service credit percentage
Equal to or greater than 99.0% but less than 99.9%	5%
Less than 99.0%	10%

Code42 will apply Service Credits against your next payment to Code42 for the Code42 Offering. If your Code42 Offering subscription expires without renewal, Code42 will promptly issue you a refund for any outstanding Service Credits. Service Credits will not entitle you to any other refund or payment from Code42 and may not be transferred or applied to any other account. Service Credits are your sole and exclusive remedy for any unavailability, nonperformance, or other failure by Code42 to provide the Code42 Offering.

4. Credit request and payment procedures

You must request a Service Credit by sending an email to [support@code42.com \(mailto:support@code42.com\)](mailto:support@code42.com) with the subject of "Service Credit Request." You must submit your Service Credit request by the end of the second calendar month following that in which Code42 failed to meet the Availability commitment. For example, if an incident occurred on January 1st, you must notify Code42 by March 31st.

Your request must include (1) a detailed description of the incident, (2) information regarding the time and duration in which the Code42 Offering was not Available, (3) the number and locations of affected Authorized Users, if available, and (4) descriptions of your attempts to resolve the incident at the time of occurrence.

Code42 will evaluate your claim using all reasonably available information and make a good faith determination of whether Code42 met its Availability commitment. If Code42 determines that it did not provide the Code42 Offering within the Availability commitment, then Code42 will issue the Service Credit during the month following that in which Code42 confirmed your request. For example, if Code42 confirms on March 15th that it did not meet its Availability commitment, Code42 will issue you a Service Credit by April 30th.

5. Service credit exclusions

The Availability commitment does not apply to any unavailability of the Code42 Offering that results from: (1) your failure to operate the Software or the Code42 Offering in accordance with the Documentation; (2) Code42's scheduled maintenance (details available at https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Scheduled_maintenance (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Scheduled_maintenance)); (3) factors outside of Code42's reasonable control, including any force majeure event or Internet access or related problems beyond the border router of Code42 datacenter; (4) equipment, software or other technology not provided or controlled by Code42; or (5) Code42's termination or suspension in accordance with the terms of the Agreement.

Exhibit □



Code42 enterprise support policy

Overview

This policy document describes □Support Services,□the procedures that Code42 Software (also referred to here as □Code42,□we,□or □us□) follows to help our enterprise customers (□you□) use our enterprise software. Our Support Services are divided into multiple subscription options (□support plans□). □e have a specific name for the team of people who provide the Support Services to you: □Customer Champions.□

This document explains:

- □ich Support Services are included in each support plan
- □hen and how you can contact our Customer Champions
- □ow we define the priority level of each issue
- □ow you can escalate an issue

This document applies only to our enterprise customers. Small business customers can refer to [CrashPlan for Small □usiness support policy \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/CrashPlan_for_Small □usiness support policy\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/CrashPlan_for_Small_business_support_policy).

Support plans

Code42 offers the following support plans, depending on your subscription:

- Code42 Select Support (previously Silver)
- Code42 Premier Support (previously Gold)
- Code42 Premier Plus Support (previously Platinum)

Support services

Each support plan includes a certain set of Support Services. This table explains which Support Services are included and which Support Services are not included in each support plan.

Support Service	Code42 Select Support (previously Silver)	Code42 Premier Support (previously Gold)	Code42 Premier Plus Support (previously Platinum)
Access to self-service documentation	Yes	Yes	Yes
Access to user forums	Yes	Yes	Yes
Issue reporting options	Web only	<ul style="list-style-type: none"> Web Chat Phone (Toll number provided) 	<ul style="list-style-type: none"> Web Chat Phone (Toll number provided)
Administrators who can contact Customer Champions	1	4	10
Consultation or pre-planning and best practices	No	Yes	Yes
Access to named Technical Account Manager (TAM) https://support.code42.com/terms-and-conditions/Code42_customer_support_resources/technical_account_manager_details	No	No	Yes

Administrator must be recognized as an administrative support contact in the support system. To be registered as an administrative support contact, email your Customer Success Manager or [create a ticket \(https://gethelp.code42.com/\)](https://gethelp.code42.com/).

Contact hours and response times

Your support plan affects the times our Customer Champions are available to you and the speed of their response to your issues.

Support Service	Code42 Select Support [previously Silver]	Code42 Premier Support [previously Gold]	Code42 Premier Plus Support [previously Platinum]
Support contact hours	<ul style="list-style-type: none"> All issues: Monday to Friday, 8:00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 8:00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 8:00 a.m. to 5:00 p.m. US CT
Support contact hours on holidays	<ul style="list-style-type: none"> All issues: We respond to issues after the holiday. 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: We respond to issues after the holiday. 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: We respond to issues after the holiday.
Response time for urgent priority issues	1 business day	1 hour	30 minutes
Response time for high priority issues	1 business day	4 hours	4 hours
Response time for normal priority issues	1 business day	1 business day	1 business day
Response time for Low priority issues	3 business days	3 business days	3 business days

Our [definitions of issue priority](#) are provided below.

Time Zones

The time zones for these support contact hours vary depending on your location.

Our Location	
USA	US Central Time (UTC-05:00 or UTC-06:00 (https://support.code42.com/Time), depending on daylight saving time)

Time for Support Contact Hours

Our Location	Time for Support Contact Hours
Europe	Eastern European Time (UTC+00:00)
Asia	Eastern European Time (UTC+00:00)
Other locations	US Central Time (UTC-05:00 or UTC-06:00, depending on daylight saving time)

Of course, support contact hours that are 24 hours a day, 7 days a week are not affected by time zones.

Support on US Holidays

Because fewer Customer Champions are available on US holidays, we prioritize issues differently, depending on your support plan and the priority of your issue.

We observe US holidays from 12:00 a.m. to 11:59 p.m., US Central Time, on the following dates:

U.S. Holiday	Date of Observance
New Year's Day	January 1
Presidents' Day	Varies (third Monday in February)
Memorial Day	Varies (last Monday in May)
Independence Day	July 4
Labor Day	Varies (first Monday in September)
Veterans Day	November 11
Thanksgiving Day	Varies (fourth Thursday in November)
Day after Thanksgiving Day	Varies (Friday after Thanksgiving Day)
Christmas Eve	December 24
Christmas Day	December 25

Our responsibility or response times

We expect you to help us to resolve your issue when we make a reasonable request for your help. If you do not answer our requests or provide assistance, we may be unable to respond to your issues according to these response times.

Support for managed appliances and monitored authorities

If you use server hardware sold and supported by Code42 (managed appliances), or if you use a monitored private authority, your Support Services and your responsibilities are also affected by our [Appliance maintenance addendum \(https://support.code42.com/Terms_and_conditions/Legal_terms_and_conditions/Appliance_maintenance_addendum\)](https://support.code42.com/Terms_and_conditions/Legal_terms_and_conditions/Appliance_maintenance_addendum). If you do not follow the guidelines in that policy, we may be unable to respond to your issues according to these response times.

Contact Code42 for enterprise support

These guidelines show how to contact us for Support Services.

Contact information

The table below provides a quick summary of the contact information for our Support Services.

Support method	Contact information
Web support	<p>Submit a ticket or check ticket status (https://gethelp.code42.com)</p> <p>You must register at https://gethelp.code42.com (https://gethelp.code42.com/) to create a case.</p>
Chat support	<p>Chat now (https://gethelp.code42.com)</p> <p>You must register at https://gethelp.code42.com (https://gethelp.code42.com/) to initiate a chat.</p>
Email support	<p>gethelp (mailto:gethelp@code42.com) @code42.com (mailto:gethelp@code42.com)</p> <p>Universities and partners should instead use chat or create a case using https://gethelp.code42.com (https://gethelp.code42.com/).</p>
Phone support	<p>Sign in to https://gethelp.code42.com (https://gethelp.code42.com/). The Call box shows the phone numbers for your support plan.</p>

How to report issues

Depending on your support plan, you can report issues to us through these three methods:

https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_enterprise_support_policy (ht

Updated: Wed, 06 Apr 2022 19:12:40 GMT

Powered by 



- eb-based ticketing
- Online chat
- Phone

Administrative support contact

To report issues, you must be recognized as an administrative support contact in the support system. To be registered as an administrative support contact, email your Customer Success Manager or [create a ticket \(https://gethelp.code42.com/\)](https://gethelp.code42.com/).

eb-based ticket

You can use Code42's web-based support ticket service to [submit a ticket \(https://gethelp.code42.com\)](https://gethelp.code42.com/) or [check the status of an existing ticket \(https://gethelp.code42.com\)](https://gethelp.code42.com/).

Online chat

Click the **Contact Support** button anywhere on the support website to [chat online with a Customer Champion \(https://gethelp.code42.com\)](https://gethelp.code42.com/).

Phone

Call Code42 for support if your issue is urgent, such as an issue that interferes with restoring files, prevents you from adopting a device, or critically affects a large number of users.

To find the phone number to call, sign in to [https://gethelp.code42.com \(https://gethelp.code42.com/\)](https://gethelp.code42.com/) and refer to the **Call s** box. Please have your registration key and email address on hand for identification purposes.

Exchange of information about support issues

Each time you report an issue, we exchange the following information with you:

- We give you an identification number that is used to reference your specific issue in the future.
- You should give us the following information in order to help us efficiently diagnose your issue:
 - **Product name** (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Identify_your_product)
 - **Operating system** and version
 - **Software version** of the [Code42 app \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Identify_version\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Identify_version)
 - **Computer ID** ([GUID \(https://support.code42.com/Incydr/Agent/Configuring/Computer_identities_how_they_work](https://support.code42.com/Incydr/Agent/Configuring/Computer_identities_how_they_work) [here is my computer identity.3F](https://support.code42.com/Incydr/Agent/Configuring/Computer_identities_how_they_work)) of affected devices

https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_enterprise_support_policy (ht

Updated: ed, 06 Apr 2022 19:12:4 GMT

Powered by  mindtouch™



- [Logs \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Send_logs_to_enterprise_support\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Send_logs_to_enterprise_support)
- **username** (or email address) of affected user accounts
- **detailed description** of the question or problem
- **Screenshots** of relevant settings or error messages
- Tell us if you are using any of our **Code42 cloud services**

Definitions of issue priority

Each time you report an issue to us, we categorize it by the priority of the issue and the potential impact to you. These are the guidelines we use to categorize the priority of each issue:

Priority Level	Description Criteria
<input type="checkbox"/> urgent	<p>The issue causes a complete loss of service and you cannot reasonably continue using the software in this state, or the issue affects your entire deployment.</p> <p>Code42 expects you to be readily available 24/7 to drive a timely resolution to the issue.</p> <p>Examples of urgent priority issues include:</p> <ul style="list-style-type: none"> • Security reporting or alerting is non-functional • Inability to restore across your deployment • Inability to back up or restore due to a licensing issue • An upgrade problem resulting in an outage

Priority Level	Description Criteria
High	<p>The issue causes a severe loss of service or affects the majority of your deployment. You can continue work in a limited capacity, but you may have an alternative method or workaround for the issue. The issue interferes with long-term use of the software.</p> <p>Examples of high priority issues include:</p> <ul style="list-style-type: none"> • Security reporting or alerting is inconsistent • Inability to restore from many devices • An installation issue • Severe performance degradation affecting your service • Inability to renew your account • An outage affecting a major portion of your deployment
Normal	<p>The issue causes a minor loss of service or affects a small portion of your deployment. You can continue work despite an inconvenience or non-critical issue with the software.</p> <p>Examples of normal priority issues include:</p> <ul style="list-style-type: none"> • An issue affecting a single user • A problem with backup reports • A problem with file exclusions • A cosmetic issue with the Code42 app or Code42 console
Low	<p>The issue causes little to no loss of service.</p> <p>Examples of low priority issues include:</p> <ul style="list-style-type: none"> • A request for additional information • A report of an error in the product documentation • A request for an additional feature or future improvement • Any issue on an unsupported version or unsupported configuration

Escalate an issue to another Customer Champion

After contacting us with a support issue, you can request that another Customer Champion handle your issue. Transferring the issue to another Customer Champion is called **escalation**. When issues are escalated, they are usually (but not always) transferred to a Customer Champion who has more experience handling issues of that type.

Include the following information:

- Your ticket number
- The reason for escalation
- The expected priority of the issue
- Additional contact information, if necessary

How we respond to an escalation request

A Customer Champion manager:

1. Evaluates your request as quickly and efficiently as possible
2. Determines an appropriate action
3. Communicates the decision to you

The manager may ask to have a direct conversation with you. Your issue may be transferred to another Customer Champion, depending on the manager's decision.

Support for version and product end-of-life

Software version support

If a software version is no longer generally available, support is provided during the end-of-life period according to the terms of your support plan.

- Full support is available for 12 months (at a minimum) following the general availability announcement of a new version (not including maintenance and patch versions).
- End-of-life announcements begin approximately six months prior to the end-of-life date. During this time we will only provide security-related fixes.

Code42 may terminate support for a software version prior to the expiration of the support period if necessary to preserve security. Code42 will notify affected customers via email and forum posts whenever it changes the support period. In cases of significant vulnerability to Code42 environments running older versions, Code42 reserves the right to push critical updates to customers or deny access to the Code42 cloud.

Customers not upgraded to a generally available Code42 software version may experience issues including, but not limited to:

- Performance degradation
- Exposure to security vulnerabilities
- Inability to connect to Code42 cloud (including on-site authority servers)
- Potential data loss

For more information about our supported versions, see the [Code42 on-premises version policy](https://support.code42.com/Terms_and_conditions/Product_lifecycle_policy/Code42_on-premises_version_policy) (https://support.code42.com/Terms_and_conditions/Product_lifecycle_policy/Code42_on-premises_version_policy).

Hardware support

If a hardware product is generally available and you have purchased [annual support on such hardware](#), the support provided during the end-of-life period is provided for up to 5 years from the hardware date of purchase.

Support provided for hardware during the end-of-life period includes:

- Hardware warranty
- Escalations
- Paths
- Maintenance releases
- Product updates
- Content updates
- Available maintenance and technical support

To receive hardware support, Code42 may require the installation of the latest software, firmware, and content updates. These elements are introduced by Code42 to add features and resolve issues. If any element is not at a current version, the total product configuration, including any software, may not be supported. Code42 will provide a version of software that includes the features outlined in the release notes for the product.

Other information about our support services

- To receive these Support Services, you must have a current subscription agreement with Code42 or one of its authorized resellers.
- Refer to your agreement with Code42 for any definitions or details that are not clearly specified in this document.

Related topics

- [Terms and conditions \(https://support.code42.com/Terms_and_conditions\)](https://support.code42.com/Terms_and_conditions)

- [CrashPlan for Small business support policy \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/CrashPlan_for_Small_business_support_policy\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/CrashPlan_for_Small_business_support_policy)
- [Contact support: create a ticket, chat, or call \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Get_support_for_CrashPlan_for_Small_business_or_Code42_CrashPlan\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Get_support_for_CrashPlan_for_Small_business_or_Code42_CrashPlan)
- [Read Code42 app log files \(https://support.code42.com/Incydr/Agent/Troubleshooting/Read_Code42_app_log_files\)](https://support.code42.com/Incydr/Agent/Troubleshooting/Read_Code42_app_log_files)

Exhibit C



Information security addendum

Effective February 1, 2022

This Information Security Addendum (“**ISA**”) applies whenever it is incorporated by reference into the Master Services Agreement between you and Code42 (“**Agreement**”). Capitalized terms used but not defined in this ISA have the meanings ascribed in the Agreement.

1. Purpose

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

1.2 Code42 follows AICPA guidelines and regularly reviews controls as described in Code42’s SOC2 independent auditor report (the “**SOC2 Report**”). For your convenience, Code42 references some of the applicable SOC2 controls in this ISA. See the SOC2 Report for exact language. Code42 will provide you with a copy of the SOC2 Report upon request.

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

2. Encryption and key management

2.1 Code42 uses industry-standard encryption techniques to encrypt Customer Data at rest and in transit (SOC: C-10).

2.2 The Code42 system is configured by default to encrypt your files at the source using AES 256-bit encryption (SOC: C-11). All connections are authenticated and encrypted using industry standard encryption technology (SOC: C-11).

2.3 Transmitted Customer Data is check-summed at the destination during the collection process (SOC: C-9).

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 (SOC: CM-11).

4. Incident response and notification

4.1 “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.

4.2 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 (SOC: OPS-4).

4.3 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 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

5.1 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 Customer Data and (C) is appropriate to the nature, size and complexity of Code42’s business operations.

5.2 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 (SOC: ORG-2).

5.3 Security Officer The Code42 Chief Information Security Officer and security governance group develop, maintain, review and approve Code42 Security Policies.

5.4 Security Training and Awareness All Code42 personnel are required to complete security awareness training at least annually (SOC: ORG-3). Code42 conducts periodic security awareness education to give personnel direction for creating and maintaining a secure workplace. (SOC: COM-11).

6. Risk management

6.1 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 (SOC: RM-1). Executive management is kept apprised of the risk posture of the organization.

☐2 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 (SOC: RM-2).

☐ Access control program

☐☐☐ 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 (SOC: LA-1).

☐2 Code42 classifies informational assets in accordance with the Code42 data classification guideline (SOC: C-5).

☐ User access management

☐☐☐ Access to Code42 systems and networks is disabled promptly upon notification of termination (SOC: LA-☐).

☐2 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 (SOC: LA-☐).

☐☐☐ Code42 uses separate administrative accounts to perform privileged functions, and accounts are restricted to authorized personnel (SOC: LA-9).

9. 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 (SOC: LA-2).

10. Remote access and cloud access

Remote access to the corporate network is secured through a virtual private network (☐PN) solution with two-factor authentication (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 ☐mp box server (SOC: LA-4).

11. 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 antivirus agent does not check in for prolonged periods of time. Issues are investigated and remediated as appropriate.

Viruses definition updates are automatically pushed out to endpoint devices from the EDR technology as they become available. (SOC: LA-11). 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 (SOC: LA-12). Code42 maintains and regularly updates an inventory of corporate and cloud infrastructure assets, and systematically reconciles the asset inventory annually (SOC: OPS-5).

12. Threat and vulnerability management and security testing

Code42's Threat and Vulnerability Management (TVM) program monitors for vulnerabilities on an on-going basis (SOC: RM-3). 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). (SOC: RM-6). External penetration tests are conducted annually by an independent third party. Significant findings from these tests are evaluated, documented and remediated (SOC: RM-4).

13. Logging and monitoring

Code42 continuously monitors application, infrastructure, network, data storage space and system performance (SOC: OPS-1). 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 (SOC: OPS-2).

14. 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 (SOC: CM-1). 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 (SOC: CM-2). Following the successful completion of testing, changes are reviewed and approved by appropriate managers prior to implementation to production (SOC: CM-3). 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 (SOC: CM-9).

15. 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 (SOC: CM-4). 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 (SOC: CM-6). 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 (SOC: CM-□). Code42 utilizes a code versioning control system to maintain the integrity and security of the application source code (SOC: CM-□).

16. 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 (SOC: LA-15). 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 (SOC: LA-16). Code42's corporate and cloud networks are logically segmented by virtual local area networks (□LANs) and firewalls monitor traffic to restrict access to authorized users, systems and services (SOC: LA-1□).

1□. Third party security

Code42 assesses and manages the risks associated with existing and new third party vendors. Code42 employs a riskbased scoring model for each third party (SOC: MON-2). Code42 requires third parties to enter into contractual commitments that contain security, availability, processing integrity and confidentiality requirements and operational responsibilities as necessary (SOC: COM-9). 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 (SOC: MON-3).

1□. Physical security

Code42 grants access to data centers and Code42 offices by □b responsibility, and access is removed as part of the Code42 separation or internal □b transfer process when access is no longer required (SOC: LA-21□SOC: LA-22).

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 (SOC: LA-23).

19. 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 (SOC: MON-1). 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.

20. 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 annually by the Chief Information Security Officer (SOC: A-5). 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 issues identified are tracked to remediation (SOC: A-6).

21. 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 (SOC: ORG-5). Code42 requires personnel to sign a confidentiality agreement as a condition of employment (SOC: C-2). Code42 maintains a disciplinary process to take action against personnel that do not comply with company policies, including Code42 security policies (SOC: ORG-3).

Exhibit D



Data processing addendum

Effective February 24, 2022

This Data Processing Addendum (“DPA”) applies whenever it is incorporated by reference into the Master Services Agreement (“Agreement”) between you and Code42. Capitalized terms used but not defined in this DPA have the meanings given to them in the Agreement.

1. Purpose and scope

In the course of providing the Offerings to you under the Agreement, Code42 will Process Customer Data on your behalf. Customer Data may include Personal Data. This DPA reflects the parties’ agreement relating to the Processing of Customer Data in accordance with the requirements of Data Protection Laws. This DPA will control in the event of any conflict with the Agreement.

2. Definitions

2.1 “CCPA” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* as amended from time to time.

2.2 “Data Controller” means the entity that determines the purposes and means of Processing of Personal Data.

2.3 “Data Processor” means the entity that Processes Personal Data on behalf of the Data Controller, including as applicable any “service provider” as that term is defined in the CCPA.

2.4 “Data Protection Laws” means any applicable data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including the applicable laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, and the United States and its states. [Ordering Activity agrees to comply with Federal Data Protection Laws of the United States, but shall not be bound by obligations of European Union, the European Economic Area and their member states, Switzerland.](#)

2.5 “Data Subject” means the individual to whom Personal Data relates.

2.6 “Personal Data” means any information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, to an identified or identifiable individual.

2 **“Processing”, “Processes” or “Process”** means any operation or set of operations performed upon Personal Data whether or not by automated means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction.

https://support.code42.com/Terms_and_conditions/Legal_terms_and_conditions/Data_processing_addendum (<https://support...>)

2 **“Standard Contractual Clauses”** means the controller to processor standard contractual clauses for transfers of personal data to third countries which do not show an adequate level of data protection (i) as approved by the European Commission decision 2021/914, dated 4 June 2021, or (ii) for transfer transfers from the United Kingdom, as approved by the European Commission decision 2010/87/EC, dated 5 February 2010 (the “**SCCs**”).

2 **“Subprocessor”** means Code42’s Affiliates or other third-party service providers that Process Customer Data for Code42.

3. Processing of customer data

Data Processing Roles As between you and Code42, you are the Data Controller of Customer Data and Code42 is the Data Processor. You control the categories of Data Subjects and Personal Data Processed under the Agreement and provide such Personal Data to Code42 for business purposes only. Code42 has no knowledge of, or control over, the Personal Data that you provide for Processing. You are solely responsible for the accuracy, quality, and legality of the Customer Data and the means by which you acquired the Customer Data.

Data Processing Instructions This DPA and the Agreement are your complete and final instructions to Code42 for the Processing of Customer Data. You and Code42 must agree on any additional or alternate instructions. Code42 will inform you if, in Code42's opinion, your instructions violate Data Protection Laws. Code42 will process Customer Data in accordance with the Agreement (including all documents incorporated in the Agreement), and to comply with other reasonable instructions you provide to Code42 (including by email) where your instructions are consistent with the Agreement. Code42 will not sell Customer Data. Code 42 will not collect, retain, use, or disclose Customer Data (A) for any purpose other than for the specific purpose set forth in the Agreement, or (B) outside the direct business relationship between you and Code42. Code42 will disclose Customer Data if required to do so by applicable law, in which case Code42 will inform you in advance unless Code42 is prohibited from doing so. Code42 certifies that it understands and will comply with the restrictions in this section 3 (Processing of Customer Data).

4. Rights of data subjects

Correction, Blocking and Deletion If you do not have the ability to amend, block, or delete Customer Data as required by Data Protections Laws, you can provide written instructions to Code42 to act on your behalf. Code42 will follow your instructions to the extent they are technically feasible and legally permissible. You will pay Code42’s costs of providing this assistance if the assistance exceeds the services provided under the Agreement.

https://support.code42.com/Terms_and_conditions/Legal_terms_and_conditions/Data_processing_addendum (<https://support...>)

Updated: Sat, 11 Jun 2022 00:06:00 GMT

Powered by 

4.2 Data Subject Requests If permitted, Code42 will promptly notify you of any request from a Data Subject for access to, correction, amendment, or deletion of that Data Subject's Personal Data. Code42 will not respond to any Data Subject request without your prior written consent, except to confirm that the request relates to you.

4.3 Cooperation and Assistance Code42 will assist you to address any request, complaint, notice, or communication you receive relating to Code42's Processing of Customer Data received from (A) a Data Subject whose Personal Data is contained within the Customer Data, or (B) any applicable data protection authority. Code42 will also assist you with your reasonable requests for information to confirm compliance with this DPA or to conduct a privacy impact assessment. You will pay Code42's costs of providing assistance if the assistance exceeds the services provided under the Agreement.

5. Code42 personnel

5.1 Confidentiality Code42 informs its personnel engaged in the Processing of Customer Data about the confidential nature of such Customer Data. These personnel receive appropriate training on their responsibilities and are subject to written agreements with confidentiality obligations that survive the termination of their relationship with Code42.

5.2 Limitation of Access Code42 ensures that access to Customer Data is limited to those personnel who require access to Process Customer Data under the Agreement.

6. Sub-processors

6.1 Authorization You expressly authorize Code42 to use Sub-processors to perform specific services on Code42's behalf to enable Code42 to perform its obligations under the Agreement. Code42 has written agreements with its Subprocessors that contain obligations substantially similar to Code42's obligations under this DPA. Code42 is liable for any breach of this DPA caused by an act or omission of its Sub-processors.

6.2 Notice and objection Code42's current Sub-processors are listed at: <http://code42.com/r/support/dpasubprocessors> (<http://www.code42.com/r/support/dpa-subprocessors>). Code42 will publish changes to its Subprocessors to this website. You can subscribe to receive notice of any changes to Code42's Sub-processors by emailing privacynotices@code42.com (<mailto:privacynotices@code42.com>) with the subject "Subscribe" from the email address to which you want notification sent. If you subscribe, Code42 will notify you by email of new Sub-Processors before authorizing such Sub-processor(s) to process Customer Data. You have a right to reasonably object to Code42's use of a new Sub-processor by notifying Code42 in writing within 10 business days after Code42 publishes notice of a new Sub-processor. If you do so, Code42 will use reasonable efforts to change the affected Software or Cloud Service, or recommend a commercially reasonable change to your configuration or use of the affected Software or Cloud Service, to avoid Processing of Customer Data by the new Sub-processor. If Code42 is unable to make or recommend such a change within a reasonable period of time, not to exceed 60 days, you may terminate only the Subscription Term for the Software and Cloud Service that Code42 cannot provide without using the new Sub-processor. You must provide written notice of termination to Code42 in accordance with the Agreement. Code42 will promptly refund you the fees applicable to the unused portion of the Subscription Term for the terminated Software and Cloud Services offering.

□ Security

□□□ **Controls for the Protection of Customer Data** □ Code42 maintains appropriate administrative, technical and organizational safeguards to protect Customer Data from unauthorized or unlawful Processing, from accidental loss, destruction, or damage. Code42's obligations are described in the Information Security Addendum available at <http://www.code42.com/r/support/dpa-information-security-addendum> (<http://www.code42.com/r/support/dpa-information-security-addendum>).

□□ **Incident Management and Breach Notification** □ Code42 will notify you within 24 hours of becoming aware of a breach of your Customer Data. To the extent known, the notice will include (A) a description of the nature of the Personal Data breach, including the categories and approximate number of your Data Subjects concerned and the categories and approximate number of your records concerned □ (B) the name and contact details of a Code42 contact point for more information □ (C) the measures Code42 is taking to address the breach, including measures to mitigate its possible adverse effects. You can find more information about Code42's incident response procedures in the Information Security Addendum.

□ Audit

□□□ **Certifications and Audits** □ Code42 uses external auditors to verify the adequacy of its security measures. Such audits are performed at least annually by independent third party security professionals and result in the generation of a confidential audit report ("□ **Audit Report**"). Code42's certifications and Audit Report are described in the Information Security Addendum.

□□ **Customer Audits** □ Code42 will provide you a copy of the Audit Report upon request so that you can reasonably verify Code42's compliance with its obligations under this DPA. You agree that any audit right granted under Data Protection Laws will be satisfied by Code42's Audit Report. If the information in the Audit Report is insufficient to reasonably demonstrate Code42's compliance with its obligations under this DPA or an audit is required by your Supervisory Authority, Code42 will provide additional information and will allow and contribute to audits, including on-site inspections. This right does not apply to the CrashPlan for Small □ Business Offering. Any such audit will be mutually agreed upon in scope, timing and duration and occur no more than once annually. You will provide written notice to Code42 to request an on-site audit of the procedures relevant to Code42's Processing of Customer Data. The audit must be conducted during normal business hours and cannot unreasonably interfere with Code42's day-to-day operations. You will conduct the audit at your own expense and reimburse Code42 for time spent on an on-site audit at Code42's then current rates.

9. Return and deletion of customer data

Upon termination or expiration of your Subscription Term, or at any time upon your request, Code42 will delete your Customer Data in accordance with the Agreement and the Documentation. Code42 will provide a certificate of deletion upon request. The Software and Cloud Services allow you to retrieve Customer Data at any time prior to the end of a Subscription Term. Providing this functionality through the Software and Cloud Services during the Subscription Term satisfies any obligation of Code42 to return Customer Data.

<https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum> (<https://support...>)

Updated: Sat, 11 Jun 2022 00:06:00 GMT

Powered by  mindtouch™



10. Transfer mechanism

To the extent Code42's processing of Customer Data requires the transfer of Personal Data from the European Economic Area, Switzerland and/or the United Kingdom to a third country that does not ensure an adequate level of protection under Data Protection Laws, such transfers will be governed by the Standard Contractual Clauses, which the parties hereby enter into and incorporate into this DPA. The parties agree that Annex I and II of the Standard Contractual Clauses attached hereto in Schedule 1 serve as Appendix 1 and 2 of the UK SCCs.

Schedule 1

Standard Contractual Clauses

Controller to Processor

Section I

Clause 1 Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
- (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Object and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 2(2) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or

[https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum \(https://support...](https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum (https://support...)

Updated: Sat, 11 Jun 2022 00:06:00 GMT

Powered by  mindtouch

to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 10 Third party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7
- (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e)
- (iii) Clause 9(a), (c), (d) and (e)
- (iv) Clause 12(a), (d) and (f)
- (v) Clause 13
- (vi) Clause 15.1(c), (d) and (e)
- (vii) Clause 16(e)
- (viii) Clause 17(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 11 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 1 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.

Clause 2 Optional blocking clause

Not applicable.

Section II Obligations of the Parties

Clause 3 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a)

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Here, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation of (EU) 2016/679 with respect to the processing in question

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with inquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 1.1.3 Use of sub-processors

(a) GENERAL WRITTEN AUTHORIZATION The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 15 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 1.1. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 1.1.4 Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the

appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13

(ii) refer the dispute to the competent courts within the meaning of Clause 1

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 10(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on

behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2017/1025, as applicable.

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 10.3 Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to inquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Section III Local laws and obligations in case of access by public authorities

Clause 4 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used, intended onward transfers, the type of recipient, the purpose of processing, the categories and format of the transferred personal data, the economic sector in which the transfer occurs, the storage location of the data transferred,

(ii) the laws and practices of the third country of destination – including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards,

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory

authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

□ here the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses □ such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided □ or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination □ such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) □ here permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. □ hen challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided

on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section I Final provisions

Clause 10 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension

(ii) the data importer is in substantial or persistent breach of these Clauses or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 10 governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 11

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Germany.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex I to the Standard Contractual Clauses

1. List of Parties

1.1 Data exporter

Name The data exporter is the customer that is party to the Agreement with Code42 Software, Inc.

Address The address associated with data exporter's Code42 account or as otherwise specified in the DPA or Agreement.

Contact details The contact details associated with the data exporter's account, or as otherwise specified in the DPA or Agreement.

Activities relevant to the data transferred under the clauses The activities specified in Section 3 of the DPA

Role controller/processor Controller

Signature and date The data exporter is deemed to have signed this Annex I by signing the Agreement or the Addendum or by using the Services.

1.2 Data importer

[https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum \(https://support...](https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum (https://support...)

Updated: Sat, 11 Jun 2022 00:06:00 GMT

Powered by 

Name The data importer is Code42 Software, Inc., a global provider of data security and endpoint data storage services.

Address 100 Washington Avenue S, Suite 2000, Minneapolis, MN 55401, United States.

Contact details General Counsel [privacy@code42.com \(mailto:privacy@code42.com\)](mailto:privacy@code42.com).

Activities relevant to the data transferred under the clauses The activities specified in Section 3 of the DPA.

Role controller processor Processor

Signature and date By signing the Agreement or the DPA, or by transferring Customer Data to third countries, the data exporter will be deemed to have signed this Annex I.

Description of the transfer

Categories of data subjects

The categories of data subjects whose personal data may be processed include: data exporter's employees, consultants, contractors, agents, prospects, customers, vendors, business partners and users authorized to use the Services; employees or contacts of third parties data exporter conducts business with.

Categories of personal data transferred

The personal data transferred may include the following categories of data: first and last name, employer, professional title, contact information (email, phone number, physical address), username, identification data (IP address, device ID) and any other personal data provided through the services; depending on the data exporter's endpoint environment and naming conventions, data transferred may include personal data, such as that possibly found in a computer name, user name or file name.

Sensitive data transferred if appropriate

The personal data transferred may include sensitive personal data, the extent of which is determined and controlled solely by the data exporter, and which may include: racial or ethnic origin; political opinions, religious or philosophical beliefs; trade-union membership; genetic or biometric data; health data; and data concerning sex-life or sexual orientation.

Frequency of the transfer e.g. whether the data is transferred on a one-off or continuous basis

Personal data is transferred in accordance with the data exporter's instructions as described in Section 3 of the DPA.

Nature of the Processing

The personal data will be processed for purposes of providing the services as described in the Agreement. The personal data transferred may be subject to the following basic processing activities: cloud based storage, retrieval, erasure or destruction, disclosure by transmission, analysis and any other processing necessary to provide and improve the

[https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum \(https://support...](https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum (https://support...)

Updated: Sat, 11 Jun 2022 00:06:00 GMT

Powered by 

services pursuant to the Agreement; to provide technical support; and otherwise in accordance with the data exporter's instructions or to comply with law.

Purpose s of the data transfer and further processing

To provide the Services under the Agreement.

The period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period

The duration of processing will be as specified and in accordance with the published data retention policies under the Agreement.

For transfers to sub-processors also specify subject matter, nature and duration of the processing

The personal data transferred may be disclosed to sub-processors of data importer solely as permitted by data importer to provide the services to data exporter under the Agreement, a current list of which is available at: <http://code42.com/r/support/dpa-subprocessors> (<http://www.code42.com/r/support/dpa-subprocessors>)

Competent supervisory authority

The data exporter's competent supervisory authority will be determined in accordance with the General Data Protection Regulation.

Annex II

A description of the technical and organizational security measures implemented by the data importer to ensure the security of Customer Data. Any capitalized term not otherwise defined herein shall have the meaning given in the Agreement.

Information Security Program

Code42 maintains a written security program appropriate to the nature, size and complexity of Code42's business operations. The program complies with industry recognized information security frameworks, and includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data. The Code42 Chief Information Security Officer and security governance group continually review and update the security program policies, standards and operating procedures to ensure it retains relevancy and accuracy.

2 System and Network Security

- a. Networks are logically segmented by virtual Local Area Networks (vLANs) and firewalls monitor traffic to restrict access to authorized users, systems and services.
- b. Firewall changes follow established processes and must be reviewed and approved.

- c. Personnel access to Code42 systems and networks is based on job responsibility. Access is promptly disabled when no longer required.
- d. Network perimeter defense solutions including an Intrusion Detection System (IDS) and firewalls are in place to monitor, detect, and prevent malicious network activity. Security personnel monitor items detected and take action as appropriate.

Server and Endpoint Security

- a. An endpoint management solution tool is used to deploy end user devices and monitor software installed on endpoints.
- b. Technology on Code42 workstations monitor for virus and malware infections. Endpoint devices are scanned in real-time. Virus definition updates are pushed to endpoint devices automatically.
- c. Cloud servers are built using industry standard security configuration management tools to set and enforce server security configurations based on industry leading practices. Servers check in hourly for configuration updates.
- d. Virtual servers are configured using a solution and adhere to the Code42 server security configuration requirements. Access to the solution is restricted to authorized individuals. Creation, modification, and removal of virtual servers requires appropriate authorizations.

4 User Access Controls

- a. Code42 personnel are required to identify and authenticate to the network with their unique user ID and password. Access to the Code42 network is secured through VPN with two-factor authentication. Password requirements are defined and enforced via a password tool.
- b. Access to cloud systems is restricted to authorized individuals. Baseline password requirements for these systems are that passwords must:
 - i. Be at least 14 characters in length
 - ii. Complexity rule – contain 3 of the 4 (uppercase, lowercase, numbers, non-alphabetic characters)
 - iii. Expire every 60 days
- c. Code42 enforces the rule of least privilege by requiring application, database, network and system administrators to restrict user access to only that needed to perform authorized functions. Successful and unsuccessful login attempts are logged.
- d. Code42 performs audits of administrator access to confidential and restricted systems, including the cloud production environment, on a regular basis. Any access by personnel who no longer require access based on job role is removed promptly.
- e. Customers are required to enter a unique account user ID and a password to access the Code42 System. The Code42 system includes additional security configuration settings within the application, including MFA for administrator console access and integration with customer-specified authentication solutions.

[https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum \(https://support...](https://support.code42.com/Terms and conditions/Legal terms and conditions/Data processing addendum)

Updated: Sat, 11 Jun 2022 00:06:00 GMT

Powered by 

Physical Security

Access to data centers is granted by job responsibilities and is removed or changed as part of the separation and internal job transfer processes. Code42 evaluates the physical security controls and assurance reports of data centers at least annually. The impact of any issues identified is assessed and remediated by the security team.

Storage and Transmission Security

- a. Industry-standard encryption technologies are used for data contained within, accessed by, or transmitted through the Code42 system. Customer data is encrypted using AES 256-bit encryption.
- b. Encryption keys are stored and transferred securely during the sign-in process using industry standard encryption technology.
- c. Customer file data transmitted to Code42 is MD5 check-summed at multiple points after encryption at the source to provide destinations the ability to detect tampering or corruption.
- d. Code42 has implemented a secure web-based data transfer tool used to encrypt and send data between customers and Code42 during customer support.

Monitoring and Logging

- a. Code42 monitors server, storage, and network devices on a real-time basis for operational performance, capacity, and availability metrics. System dashboards are configured to alert when pre-defined thresholds are exceeded.
- b. Incident management and escalation procedures exist to address system issues, problems and security-related events, in a timely manner. Incidents are logged, prioritized, and resolved based on established criteria and severity levels.
- c. Code42 utilizes a security information event monitoring (SIEM) system to pull real-time security log information from servers, firewalls, routers, intrusion detection system devices, end users, and administrator activity. The SIEM is configured for alerts and monitored on an ongoing basis. Logs contain details on the date, time, source, and type of events and are reviewed by the security team.

Software and Application Security

- a. Code42 has established a Software Development Life Cycle (SDLC) process to govern the acquisition, development, implementation, configuration, maintenance, modification, and management of infrastructure and software components.
- b. Code42 utilizes a code versioning control system to maintain the integrity and security of the application source code.
- c. Product releases 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.
- d. Monthly internal and external vulnerability scans are conducted using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated and remediated to address the associated risk(s).

- e. External application penetration tests are conducted by an independent third party at least annually. Critical findings from these tests are evaluated, documented and remediated.

☐☐ Instructions to Personnel

- a. All personnel sign a confidentiality agreement as part of their employment contract.
- b. All personnel are required to complete security training upon hire and on an annual basis. Security training includes, at a minimum:
 - i. Security education and communications.
 - ii. General and role-specific security training.
 - iii. Ongoing phishing tests.
 - iv. Instructions on how to report security incidents.
 - v. Responsibilities regarding data privacy and security.
- c. Upon hire and annually thereafter, all personnel must review and acknowledge the security program policies, standards, and operating procedures related to security, availability, processing integrity and confidentiality.

☐☐☐☐ Ensuring Availability

- a. To meet customer availability commitments, future processing demand is forecasted, compared to protected capacity demand and reviewed weekly and evaluated by the Cloud Operations department for corrective actions, if needed.
- b. Weekly maintenance windows exist for both system maintenance (Code42 cloud infrastructure) and release maintenance (new features, enhancements, and fixed to Code42 products). Details for scheduled maintenance and any disruption of service are posted on the Code42 status page.
- c. A customer critical response meeting is conducted daily to monitor and review any critical or system performance issues that may impact customers.
- d. Code42 maintains a business continuity plan and a disaster recovery plan to manage significant disruptions to Code42 operations and infrastructure. The plans are updated as needed, but at least annually, and approved by the Chief Information Security Officer.

☐☐☐ Certifications and Assessments

Code42 conducts third party audits to attest to various frameworks including ISO 2001, SOC2 Type 2, and application penetration testing.

2 Data Storage and Erasure

Customer data collected by Incydr Professional or Enterprise is retained for a period of 90 days, unless the customer uses functionality in the product to retain certain data for a longer period of time. For CrashPlan and Incydr Basic or Advanced, file activity data is retained for 90 days, and customer files are retained for the duration that Code42 provides the Services. All customer data is permanently deleted within 90 days of termination in accordance with industry recognized standards for data destruction.

3 Subprocessor Compliance

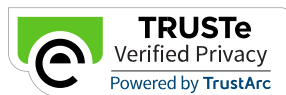
Code42 has an established process to assess and manage third party sub-processors. All sub-processors are contractually obligated to comply with the security requirements established in this Annex, or in any event, requirements that are substantially similar or equivalent. The security team performs a security review of sub-processors during an onboarding process and at least annually thereafter.



Contact Sales



Code42 Privacy Statement



Effective: August 2, 2021

Code42 Software, Inc. (“Code42”) knows that you care about your personal data, and your privacy is important to us. This Privacy Statement describes the personal data we collect and how we use or share that data. It also explains your rights regarding our processing of your personal data.

This Privacy Statement applies to personal data collected by us through a Code42 website, in connection with our events, and sales and marketing activities, and from customers of our products and services where we act as a controller of the personal data. Please see our [Applicant Privacy Statement](#) for information on personal data we collect about job applicants. This Privacy Statement provides the following information:

- . Personal data we collect
- . How we use personal data
- . When we share personal data
- . How long we retain personal data
- . When we transfer personal data internationally



- . How we secure personal data
- . Our Privacy Shield certification
- . Your privacy rights
- . Conditions of use, notices and revisions
- . Links to other sites
- . Personal data from children
- . How to contact us
- . Code42 affiliates

Contact Sales



1. Personal data we collect

The following are types of personal data we collect. The specific information we collect will depend on how you interact with Code42.

Data you provide to us. We collect personal data directly from you when:

- You enter information on our website or send to us electronically (including information you choose to provide when completing any ‘free text’ boxes in our forms) to express interest in obtaining additional information about our products and services, sign up for a webinar, event or contest, download certain content or submit survey responses.
- You attend one of our events.
- You engage with sales representatives, including during phone calls.
- You contact customer support.
- You post on our message boards, chat features, blogs and other Code42 services to which you are able to post information and materials.
- You visit our offices and register as a visitor.

The personal data you provide directly to us may include your name, address, telephone number, email address, billing information, job title, department or job role, as well as the nature of your request or communication.



You can choose not to provide some information, but doing so may limit our ability to communicate with you or fulfill your requests.

Data we collect automatically. When you interact with our website or receive electronic communications from us, we automatically collect information, including:

- Information about your device and network. This includes information about the specific device you are using, such as the hardware model, operating system version, web browser and your Internet Protocol (IP) address/MAC address/device identifier. [Contact Sales](#)
- Information through cookies, clear GIFs, pixel tags and other similar technologies This includes statistics on your activities on the website, pages accessed and links clicked; information about how you came to and used the website; broad geographic location (e.g. country or city-level location) and other technical data collected through cookies, pixel tags and other similar technologies that uniquely identify your browser; and confirmation when you open an electronic communication.

This data often does not reveal your identity directly. For additional information about our use of cookies and similar technologies, please read our [Cookie Notice](#).

Data we receive from other sources: We receive information from third parties, such as channel partners, social media platforms, joint marketing partners, referral or commercial lead sources and other data providers. In certain circumstances, we will send you an email letting you know that we have received your personal data, the source of the data, and a link to this Privacy Statement.

Personal data we receive from these sources includes name, email address, phone number, event attendance information, job role, public employment profile, and information about your product or service interests or preferences.



We may combine this information we receive from other sources with other personal data we hold about you and use it as described in this Privacy Statement.

2. How we use personal data

Code42 relies on a variety of information to operate our business. We collect and process your personal data for the following purposes. Where required by law, we obtain your consent to use and process your personal data for these purposes. Otherwise, we rely on another authorized legal basis to collect and process your personal data.

- Provide products and services to you and fulfill other requests you have, including support requests, as necessary to perform our contract with you. Where we have



not entered into a contract with you, our processing of your personal data is based on our legitimate interest to provide you with the content you request; s Evaluate the frequency, duration and patterns of usage of our website to improve the user experience. This use is necessary for our legitimate interest in understanding how users experience our website);

- Update and expand our records with new information, and analyze our records to identify potential customers by understanding your role in your organization (for EU data subjects, this use is based on your consent to receiving communication about our products and services that may be of interest to you); and
- Contact you with tailored advertising for products and services that may be of interest to you, including information about our products, promotions, and events as necessary for our legitimate interest or to the extent you have provided consent.
- Register you as a visitor to our o cces and manage non-disclosures you may be required to sign to the extent such processing is necessary for our legitimate interest in protecting our o cces and our confidential information against unauthorized access.
- Manage event registrations and attendance to plan and host events or webinars for which you have registered or that you attend, including sending related communications to you, to perform our contract with you;
- Manage contests or promotions you register for, which is necessary to perform our contract with you.

3. When we share personal data

We share your personal data as necessary to operate our business. We do not sell your personal data and do not share it except as described below.

- Code42 a liates: Code42 may use a liates that it controls (see “Code42 a liates” below) to provide products, services or support to you. We transfer your personal data to those a liates, and they will process your personal data as data controllers in accordance with this Privacy Statement.



—

- Business partners: Code42 shares your personal data with resale partners to fulfill product and information requests. We engage in joint sales or product promotions with select business partners and share your contact information with those partners if you consent to sharing when you express interest in the product or promotion.

Contact Sales

Service providers: Code42 uses other companies and individuals to provide services on its behalf, such as to assist with marketing, billing, customer support, payment processing and data analysis. These service providers have access to the personal data required to provide their services and are prohibited from using your personal data for any other purpose.

- Professional advisers: Code42 may share personal data with professional advisers acting as service providers, processors, or joint controllers – including lawyers, bankers, auditors, and insurers to the extent we are legally obliged to share or have a legitimate interest in sharing your personal data.

- Event partners: If you attend an event or webinar organized by us, Code42 may share your personal data with partners or sponsors of the event or webinar. If required by applicable law, you may consent to such sharing by opting-in via the registration form. In these circumstances, your information will be subject to the partner’s privacy statements. If you do not wish for your information to be shared you can opt-out in accordance with Section 8 below.

- Business transfers: In the event that Code42 or substantially all of its assets are acquired or Code42 is involved in a merger, dissolution, sale of all or a portion of its assets, or other fundamental corporate transaction, we reserve the right to sell or transfer your personal data as part of the transaction.

- Protection of Code42 and others: Code42 shares personal data when required by law or to respond to legal process, to protect customers or others, to maintain the security of our products, and to protect the rights or property of Code42.
- Community website and blog users: Any information that you post on our community pages or blog is publicly available



and will be accessed through search engines or other publicly available platforms. It may be “crawled” or searched by third parties.

- With your consent: Except as described above, we will provide you with notice when your personal data will be shared with third parties, and you can choose not to share that information.

4. How long we retain personal data

Code42 will retain your personal data for as long as needed to fulfill the purpose for which it is collected, and as required or permitted by law (such as tax, Contact Sales legal, accounting or other purposes). See Section 8 for information on your rights for storage of your personal data. We will consider your request in accordance with applicable laws.

5. When we transfer personal data internationally

Code42 is headquartered in the United States with entities, operations and service providers in the United States and throughout the world. Your personal data may be transferred outside your jurisdiction, including to countries that are not subject to an adequacy decision by the European Commission and that may not provide for the same level of data protection as your jurisdiction). We have appropriate safeguards to ensure your personal data receives an adequate level of protection and security. This includes entering into agreements with written assurances from services providers and implementing standard contractual clauses, as required, for the transfer of personal data as approved by the European Commission.

6. How we secure personal data

Code42 uses administrative, organizational, technical and physical safeguards to protect your personal data. We use physical access controls, encryption, Internet firewalls, intrusion detection and network monitoring depending on the type of data. We also require our service providers to use appropriate security measures. If you have questions about the security of our website, products, or services, please contact us at security@code42.com.

7. Our Privacy Shield certification

Code42 has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework regarding the collection, use and retention of personal data transferred from the European Union, United Kingdom and Switzerland. While Code42 does not rely on these frameworks for the transfer of personal data, we adhere to the Framework's applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce's Privacy Shield site at <https://www.privacyshield.gov>.

Code42 is responsible for the processing of the personal data it receives under each Privacy Shield Framework and subsequently transfers to a third party acting as a Contact Sales agent on its behalf. Code42 complies with the Privacy Shield Principles for all onward transfers of personal data, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, Code42 is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we are required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, Code42 commits to resolve complaints about our collection or use of your personal data. EU, UK and Swiss individuals with inquiries or complaints regarding our Privacy Statement should first contact Code42 at privacy@code42.com.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at <https://www.feedback-form.truste.com/watchdog/request>.



Under certain conditions, more fully described on the Privacy Shield website, you may be entitled to invoke binding arbitration by going to <https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint> when other dispute resolution procedures have been exhausted.

8. Your privacy rights

Updating your information: If you would like to update the personal data you have provided to us, please contact us at privacy@code42.com.

Marketing communications: You can opt-out of receiving marketing communications from us by clicking “unsubscribe” in any marketing email communications we send you, or by unsubscribing at <https://www.code42.com/preference/>.

Additional rights for the EEA and certain other territories: If you are located in certain territories (such as the European Economic Area and United Kingdom), you have the

right, under certain circumstances, to exercise the following privacy rights available to you under applicable data protection laws:

Contact Sales



Right not to provide consent or to withdraw consent: We rely on your consent to process certain personal data. Where we do so, you have the right not to provide your consent or to withdraw your consent at any time. You can revoke consent to receiving marketing communications from us by clicking “unsubscribe” in any marketing email communication we send you, or by unsubscribing at <https://www.code42.com/preference/>.

- You can revoke consent generally by sending an email to privacy@code42.com. Right of
- access: You have the right to access the personal data that we hold about you.
- Right of erasure: In certain circumstances, you have the right to request the deletion of your personal data.
- Right to object to processing: You have the right to request that Code42 stop processing your personal data and we will do so if we are processing your personal data for marketing, or if we are relying on our legitimate interest to process your personal data – unless we demonstrate compelling legitimate grounds to continue the processing.
- Right to data portability: You have the right to obtain the personal data that you consented to give us or that was provided to us to perform our contract with you. We will provide your personal data in a structured, commonly used and machine-readable format, and you may reuse it elsewhere.
- Right to rectification: You have the right to require us to correct any inaccurate or incomplete personal data.
- Right to restrict processing: You have the right to request that we restrict processing of your personal data in certain circumstances, to the extent permitted by applicable data laws.
- Right to lodge a complaint with the data protection authority: If you have a concern about our privacy practices, including the way we handled your personal data, you can report it to the data protection authority that is authorized to hear those concerns.

To exercise your rights, please contact privacy@code42.com. Code42 will consider your request in accordance with applicable and will respond within a reasonable timeframe. To protect your privacy and security, we will take appropriate steps to verify your identity before complying with the request.



California Privacy Right:

The California Consumer Protection Act (CCPA) provides California consumers with specific rights regarding the processing of their personal information. You have the ability to request that Code42:

- provide details about the categories of personal information that we collect about you, including how we use and share it;
- provide you access to the personal information we collect about you; and delete the
- personal information we have about you.

To exercise your rights, please contact privacy@code42.com. Code42 will consider your request in accordance with applicable law and respond within a reasonable timeframe. To protect your privacy and security, we will take appropriate steps to verify your identity before complying with the request.

9. Conditions of use, notices and revisions

If you choose to visit a Code42 website, your visit and any dispute over privacy is subject to this Privacy Statement and our website terms of use. If you have any concern about privacy at Code42, please contact us with a thorough description, and we will try to resolve it. Our business changes constantly, and our Privacy Statement will change also. We may email periodic reminders of our notices and conditions, but you should check our website frequently to see recent changes. If required by applicable law, we will notify you of any material changes to this Privacy Statement. Unless stated otherwise, our current Privacy Statement applies to all information that we have about you. We will never materially change our policies and practices to make them less protective of personal data collected in the past without the consent of affected individuals.



10. Links to other sites

Our website provides links to other websites through direct links or through applications such as “Share” or “Like” buttons. Other websites may contain links to Contact Sales the Code42 website or services. We do not control those sites or their privacy practices, which differ from those described in our Privacy Statement. The personal data you choose to give to unrelated parties is not covered by this Privacy Statement, and we encourage you to review their privacy policies.

11. Personal data from children

Our website, products and services are not directed to individuals under the age of 16. We do not knowingly collect personal data from those individuals. If you become aware that a child has provided us with personal data, please contact us in accordance with Section 12 below. If we become aware that a child under the age of 16 has provided us with personal data, we will take steps to delete the information.

12. How to contact us

If you have any questions about this Privacy Statement, you can write to us or any of our affiliates at privacy@code42.com or by mail at: privacy@code42.com or by mail at:

Code42 Software, Inc.
100 Washington Ave. S, 20th Floor
Minneapolis, MN 55401
United States
Attn: General Counsel

Our EU Data Representative is Code42 Software GmbH. You can contact our EU Data Representative at privacy@code42.com or by mail at:



Code42 Software GmbH
Johannstraße 39
40476 Düsseldorf
Deutschland
Attention: General Counsel

13. Code42 a liates



Code42 Software UK LTD
Third Floor – The Pearce Building West
Street, Maidenhead SL6 1RL
United Kingdom

Contact Sales

Code42 Software GmbH
Johannstraße 39
40476 Düsseldorf
Deutschland

Contact Sales
Request 4-Week Trial



PRODUCTS

Incydr™

Incydr Gov™

Instructor™

SOLUTIONS

Departing Employee

Data Ex ltration

Insider Threat

Detection

IP Theft Protection

Data Loss Prevention

Security Awareness

Training

INDUSTRY

Federal

Software Tech

Life Sciences

Business Services

Manufacturing

SERVICES

Overview

Advisory

Technology

Education

Support

PARTNERS

Technology

Integrations

Reseller Partners

Partner Portal

SUPPORT

Help Center

Code42 University

Customer Toolkit

CODE42

Contact Sales

Careers

News

RESOURCES

Blog

Resource Center

Glossary

Code42 Privacy Statement © 2022

Code42 Software, Inc. All rights reserved.

Exhibit F-1



Incydr Basic, Advanced, and Gov F1 product plans

Overview

This article explains which features are included in Incydr Basic, Incydr Advanced, and Incydr Gov F1 product plans. Incydr is a SaaS data risk detection and response product that allows security teams to effectively mitigate file exposure and exfiltration risks without disrupting legitimate collaboration.

If you're not sure which product plan you have, check the [Account menu \(https://support.code42.com/Incydr/Admin/Code42_console_reference/01_Code42_console_overview/Account_menu\)](https://support.code42.com/Incydr/Admin/Code42_console_reference/01_Code42_console_overview/Account_menu) from the Code42 console.

- For information about other product plans, see [Code42 product plans \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans).
- For more information about any of our product plans, contact [sales \(https://code42.com/contact\)](https://code42.com/contact) or your Customer Success Manager (CSM).
- For questions about your subscription, invoice, or bill, contact your Customer Success Manager (CSM).

At a glance

- **Incydr Basic** provides fundamental features for insider risk detection, investigation, and response.
- **Incydr Advanced** provides all of our most advanced features for insider risk detection, investigation, and response.
- **Incydr Gov F1** is the FedRAMP-authorized version of our Incydr Advanced product. For more details, see [Code42 and FedRAMP compliance \(https://support.code42.com/Terms_and_conditions/Compliance_resources/Code42_and_FedRAMP_compliance\)](https://support.code42.com/Terms_and_conditions/Compliance_resources/Code42_and_FedRAMP_compliance).

Product plan details

Symbol	Meaning
	Included in this product plan
No	Not available with this product plan

Supported risk detection sources

	Incydr Basic	Incydr Advanced	Incydr Pro
Endpoints	Windows, Mac, Linux	Windows, Mac, Linux	Windows, Mac, Linux
Business applications	Available as an add-on. Supported services: Salesforce	Available as an add-on. Supported services: Salesforce	Available as an add-on. Supported services: Salesforce
Cloud storage services	One cloud service is included. Additional cloud services can be added. Supported cloud services: Microsoft OneDrive, Google Drive, Box	One cloud service is included. Additional cloud services can be added. Supported cloud services: Microsoft OneDrive, Google Drive, Box	Available as an add-on. Supported cloud services: Microsoft OneDrive, Google Drive, Box
Email services	Available as an add-on. Supported email services: Office365, Gmail	Available as an add-on. Supported email services: Office365, Gmail	Available as an add-on.

Platform capabilities

	Incydr Basic	Incydr Advanced	Incydr Pro
Endpoint monitoring	✓	✓	✓

	Incydr Basic	Incydr Advanced	Incydr Professional
File metadata collection	No	✓	✓
Trusted activity preferences	✓	✓	✓
File collection and preservation	✓	✓	✓
Event data retention	30 days <i>Upgrade to 90 days available for purchase</i>	90 days	90 days

Features

	Incydr Basic	Incydr Advanced	Incydr Professional
Insider risk indicators File vector and user	✓	✓	✓
Hours risk indicator	No	✓	✓
Security events dashboards Risk exposure and Insider Risk trends	✓	✓	✓
Attack lists	✓	✓	✓
User activity profiles	✓	✓	✓
Alerting	✓	✓	✓

	Incydr Basic	Incydr Advanced	Incydr Overview
Forensic Search	✓	✓	✓
Download & filtered file contents	✓	✓	✓
Case management for investigations	✓	✓	✓
Extended retention of file content (legal hold)	✓	✓	✓
Code42 Instructor	Available as an add-on	Available as an add-on	Available as an add-on

Integrations

	Incydr Basic	Incydr Advanced	Incydr Overview
Code42 API	Basic access Upgrade to full access https://support.code42.com/Incydr/Admin/Monitoring_and_managing/Code42_API_resources/API_access available for purchase	✓	✓
Identity management SSO	✓	✓	✓
SaaS integrations	✓	✓	✓
SIEM integrations	✓	✓	✓

	Incydr Basic	Incydr Advanced	Incydr Professional
Incydr workflows automations	Paid service	Paid service	No

Support plans

For details about these support plans, see [Incydr support policy \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy).

	Incydr Basic	Incydr Advanced	Incydr Professional
Level	Code42 Select Support (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy#Support_plans) Upgrade to Code42 Code42 Premier Support available for purchase	Code42 Premier Support (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy#Support_plans)	Code42 Premier Support (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy#Support_plans)
Contact hours	<ul style="list-style-type: none"> All issues: Monday to Friday, 00:00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 00:00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 00:00 a.m. to 5:00 p.m. US CT
Response time	Urgent: 1 day High: 1 day Normal: 1 day Low: 3 days	Urgent: 1 hour High: 4 hours Normal: 1 day Low: 3 days	Urgent: 1 hour High: 4 hours Normal: 1 day Low: 3 days
Number of named contacts	1	4	4

	Incydr Basic	Incydr Advanced	Incydr Professional
Technical account manager	Paid service	Paid service	Paid service
ProStart	Paid service	Paid service	Paid service

Related topics

- [Code42 product plans \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans)
- [Incydr support policy \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy)
- [Policy notifications \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Policy_notifications\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Policy_notifications)
- [Code42 customer support resources \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources)

Exhibit F-2



Incydr Professional, Enterprise, Gov F2, and Horizon product plans

Overview

This article explains which features are included in Incydr Professional, Enterprise, and Horizon product plans. Incydr is a SaaS data risk detection and response product that allows security teams to effectively mitigate file exposure and exfiltration risks without disrupting legitimate collaboration.

If you're not sure which product plan you have, check the [Account menu \(https://support.code42.com/Incydr/Admin/Code42_console_reference/01_Code42_console_overviewAccount_menu\)](https://support.code42.com/Incydr/Admin/Code42_console_reference/01_Code42_console_overviewAccount_menu) from the Code42 console.


- For information about other product plans, see [Code42 product plans \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans).
- For more information about any of our product plans, contact [sales \(https://code42.com/contact\)](https://code42.com/contact) or your Customer Success Manager (CSM).
- For questions about your subscription, invoice, or bill, contact your Customer Success Manager (CSM).

At a glance

Incydr is a SaaS data risk detection and response product that allows security teams to effectively mitigate file exposure and exfiltration risks without disrupting legitimate collaboration. The Incydr Professional, Enterprise, and Horizon product plans use a streamlined version of the Code42 app that is purpose-built for insider risk management.

- **Incydr Professional** provides fundamental features for insider risk detection, investigation, and response.
- **Incydr Enterprise** provides advanced features for insider risk detection, investigation, and response.
- **Incydr Gov F2** is the FedRAMP-authorized version of our Incydr Enterprise product. For more details, see [Code42 and FedRAMP compliance \(https://support.code42.com/Terms_and_conditions/Compliance_resources/Code42_and_FedRAMP_compliance\)](https://support.code42.com/Terms_and_conditions/Compliance_resources/Code42_and_FedRAMP_compliance).
- **Incydr Horizon** provides all of our most advanced features for insider risk detection, investigation, and response.

Product plan details

Symbol	Meaning
	Included in this product plan
No	Not available with this product plan

Supported risk detection sources

	Incydr Professional	Incydr Enterprise	Incydr Gov 2	Incydr Origin
Endpoints	Windows, Mac, Linux	Windows, Mac, Linux	Windows, Mac, Linux	Windows, Mac, Linux
Business applications	Available as an add-on Supported services: Salesforce	Available as an add-on Supported services: Salesforce	Available as an add-on Supported services: Salesforce	Salesforce data connection is included

	Incydr Professional	Incydr Enterprise	Incydr ² Core	Incydr ² Enterprise
Cloud storage services	<p>One cloud service is included. Additional cloud services can be added.</p> <p>Supported cloud services: Microsoft OneDrive, Google Drive, Box</p>	<p>One cloud service is included. Additional cloud services can be added.</p> <p>Supported cloud services: Microsoft OneDrive, Google Drive, Box</p>	<p>Available as an add-on</p> <p>Supported cloud services: Microsoft OneDrive, Google Drive, Box</p>	<p>Microsoft OneDrive, Google Drive, and Box data connections are included</p>
Mail services	<p>Available as an add-on</p> <p>Supported email services: Office365, Gmail</p>	<p>Available as an add-on</p> <p>Supported email services: Office365, Gmail</p>	<p>Available as an add-on</p>	<p>Office365 and Gmail data connections are included</p>

Platform capabilities

		Incydr Professional	Incydr Enterprise	Incydr Gov 2	Incydr Orion
Endpoint monitoring		✓	✓	✓	✓
Metadata collection					
	Filtered file activity	✓	✓	✓	✓
	File activity cloud	✓	✓	Included if you have purchased a cloud or email service add-on	✓
	File activity endpoint	No	Available as an add-on	Available as an add-on	Available as an add-on
Trusted activity preferences		✓	✓	✓	✓
Event data retention		30 days <i>Upgrade to 90 days available for purchase</i>	90 days	90 days	100 days

Features

	Incydr Professional	Incydr Enterprise	Incydr Gov 2	Incydr Orion
Insider risk indicators file vector and user	✓	✓	✓	✓
Hours risk indicator	No	✓	✓	✓

	Incydr Professional	Incydr Enterprise	Incydr Gov	Incydr Orion
Security events dashboards Risk Exposure and Insider Risk Trends	✓	✓	✓	✓
Attack lists	✓	✓	✓	✓
User activity profiles	✓	✓	✓	✓
Alerting	✓	✓	✓	✓
Forensic Search	✓	✓	✓	✓
Download and filtered file contents	✓	✓	✓	✓
Case management for investigations	✓	✓	✓	✓
Code42 Instructor	Available as an add-on	Available as an add-on	Available as an add-on	Included

Integrations

	Incydr Professional	Incydr Enterprise	Incydr Gov 2
Code42 API	Basic access Upgrade to full access <i>(available for purchase)</i>	Full access	Full access
Identity management (SSO)	✓	✓	✓
SaaS integrations	✓	✓	✓
SIEM integrations	✓	✓	✓
Incydr iOS / Android automations	Paid service	1 departing employee flow included	No

Support plans

For details about these support plans, see [Incydr support policy](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy).

	Incydr Professional	Incydr Enterprise	Incydr Gov 2	Incydr Orion
Level	Code42 Select Support Code42 Premier Support Upgrade to Code42 Code42 Premier Support available for purchase	Code42 Premier Support Code42 Premier Support	Code42 Premier Support Code42 Premier Support	Code42 Premier Plus Support Code42 Premier Plus Support
Contact hours	<ul style="list-style-type: none"> All issues: Monday to Friday, 00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 00 a.m. to 5:00 p.m. US CT 	<ul style="list-style-type: none"> Urgent priority issues: 24 hours a day, 7 days a week All other issues: Monday to Friday, 00 a.m. to 5:00 p.m. US CT
Response time	Urgent: 1 day High: 1 day Normal: 1 day Low: 3 days	Urgent: 1 hour High: 4 hours Normal: 1 day Low: 3 days	Urgent: 1 hour High: 4 hours Normal: 1 day Low: 3 days	Urgent: 30 minutes High: 4 hours Normal: 1 day Low: 3 days
Number of named contacts	1	4	4	10
Technical account manager	Paid service	Paid service	Paid service	Included
ProStart	Paid service	Paid service	Paid service	Paid service

Related topics

- Code42 product plans (https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans/Incydr_Pro...)

[Code42 product plans](#))

- [Incydr support policy \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy)
- [Policy notifications \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Policy_notifications\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Policy_notifications)
- [Code42 customer support resources \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources)

Exhibit F-3



Code42 Instructor product plans

Overview

This article explains which features are included in our Code42 Instructor product plans.

Code42 Instructor provides proactive, situational, and responsive education content. If you're adding insider risk education to an existing security awareness solution, you can add Code42 Instructor lessons to your existing learning management system. Or, if you're building a standalone insider risk education program, you can use Code42 Instructor lessons in your incident response process to assign education based on user activity.

- For information about other product plans, see [Code42 product plans \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans).
- For more information about any of our product plans, contact [sales \(https://code42.com/contact\)](https://code42.com/contact) or your Customer Success Manager (CSM).
- For questions about your subscription, invoice, or bill, contact your Customer Success Manager (CSM).

At a glance

- **Code42 Instructor Lesson Packs** provide best-in-class insider risk reduction training. Lessons are tailored to help reduce insider risks proactively and responsively.
- **Code42 Custom Branded Instructor Lesson Packs** provide the same base content as Code42 Instructor Lesson Packs, but with the ability to customize lessons with your company logo and information.

Product plan details

Symbol	Meaning
	Included in this product plan
No	Not available with this product plan

Features

	Code42 Instructor Lesson Packs	Code42 Custom Branded Instructor Lesson Packs
Proactive lessons	✓	✓
Situational lessons	✓	✓
Responsive lessons	✓	✓
Custom branding	No	✓

Lesson pack contents

Proactive lessons

- Insider Risk & You
- Keeping Source Code safe
- Keeping your Marketing data safe
- Keeping your Sales data safe
- Avoiding Common Data Risks: Google Drive edition
- Avoiding Common Data Risks with Slack
- Avoiding Common Data Risks: Office365/OneDrive edition
- Avoiding Common Data Risks with iCloud

Situational lessons

- Departing Employee: Do's-and-Don'ts
- Users with Elevated Access: Avoiding common data risks
- New Employee: Do's-and-Dont's

Responsive lessons

- iCloud sync
- Google Drive - Unsafe Sharing
- Office 365 - Unsafe Sharing

- Personal Email
- Slack
- Source Code Repository
- Unapproved Cloud Service

Related topics

- [Introduction to Code42 Instructor \(https://support.code42.com/Incydr/Admin/Monitoring_and_managing/Introduction_to_Code42_Instructor\)](https://support.code42.com/Incydr/Admin/Monitoring_and_managing/Introduction_to_Code42_Instructor)
- [Code42 product plans \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_product_plans)
- [Incydr support policy \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Incydr_support_policy)
- [Policy notifications \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Policy_notifications\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Policy_notifications)
- [Code42 customer support resources \(https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources\)](https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources)