Business Associate Agreement

While Commvault does not have visibility into the nature of Customer Data due to encryption, we understand our Customers may be subject to the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act Title XIII of the American Recovery and Reinvestment Act, 2009 and regulations promulgated thereunder from time to time ("HIPAA"). To the extent Customer chooses to backup protected health information ("PHI") within the SaaS Solution, this Business Associate Agreement (the "BAA") forms part of the Master Terms and Conditions, or other agreement between Commvault and Customer for the purchase of Commvault's products and services. Any terms not defined have the same definition ascribed to them in the Master Terms and Conditions or HIPAA. Customer enters into this BAA as the Covered Entity. To execute this BAA, Customer should complete Customer's information and return the fully executed BAA to contracts@commvault.com.

1. **Obligations and Activities of Commvault.** In connection with the obligations of a Business Associate, Commvault agrees to: (a) not use or disclose PHI other than to provision the SaaS Solution, or as permitted or required by law or this BAA; (b) use reasonable and appropriate privacy and security safeguards to prevent use or disclosure of PHI as provided for by this BAA and consistent with the requirements of the Security Rule set forth at Subpart C of 45 CFR Part 164 with respect to PHI as determined by Commvault; and (c) report to Customer any use or disclosure of PHI not provided for in connection with the provision of the SaaS Solution or this BAA, of which it becomes aware, including breaches of unsecured PHI as required by 45 CFR 164.410; provided that notice is hereby deemed given for "Unsuccessful Security Incidents," defined as a security incident that does not result in the unauthorized access, use, disclosure, modification or destruction of PHI, or interference with system operations in an information system. This notice shall satisfy any notices required of Commvault to Customer of the ongoing existence and occurrence of Unsuccessful Security Incidents, for which no additional notice to Customer shall be given or required. Notification of a breach of unsecured PHI under 45 CFR 164.410 will be made without unreasonable delay, but in no event more than seventy-two (72) hours after Commvault's discovery thereof and will be delivered to Customer by means selected by Commvault, including via email (a "Notice"). Commvault's obligation of notification under this section shall not be construed as an acknowledgment by Commvault of any fault or liability with respect to any use or disclosure of PHI, or security incident or breach related thereto. Notice will include a description of the incident and the type of unsecured PHI involved. If applicable, Commvault shall ensure that, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), any of its subcontractors that create, receive, maintain, or transmit Customer's PHI on behalf of Commvault comply with restrictions, conditions, and requirements at least as stringent as those that apply to Commvault with respect to PHI. If Commvault maintains PHI in a Designated Record Set, upon Customer's request, Commvault shall provide Customer with access to the same for amendment. Commvault shall maintain and make available an accounting of disclosures (if any) to the Customer as necessary to satisfy Customer's obligations. To the extent Commvault is to carry out one or more of Customer's obligation(s) under Subpart E of 45 CFR Part 164, Commvault shall comply with the requirements of Subpart E that apply to the Customer in the performance of such obligations and make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary, for purposes of determining Customer's compliance with the HIPAA, subject to attorney-client and other applicable legal privileges.

2. **Permitted Uses and Disclosures by Commvault.** Commvault will use or disclose only the minimum necessary amount of PHI as set forth in this BAA or as required by law. Commvault shall not use or disclose PHI in any manner that would violate HIPAA if done by Customer.

   Commvault may use and disclose PHI for the proper management and administration of the SaaS Solution or to carry out Commvault's legal responsibilities, provided, the disclosures are required by law, or Commvault obtains reasonable assurances from the recipient of the information that any PHI will remain confidential, be used or further disclosed only as required by law or for the purposes for which it was disclosed to them, and the recipient shall be required to notify Commvault of any instances of which it is aware in which the confidentiality of the PHI has been breached. Commvault shall maintain an accounting of any disclosures of PHI in accordance with 45 CFR § 164.528.

3. **Provisions for Covered Entity to Inform Commvault of Privacy Practices and Restrictions.** To the extent it may affect Commvault's use or disclosure of PHI, Customer shall notify Commvault of: (i) any limitations in the notice of privacy practices of Customer under 45 CFR 164.520, (ii) any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, and (iii) any restriction on the use or disclosure of PHI that Customer has agreed to or is required to abide by under 45 CFR 164.522. Customer shall implement appropriate privacy and security safeguards to protect its PHI in compliance with HIPAA, and to protect its Customer Account details from unauthorized access. It is Customer's responsibility to ensure Customer has the appropriate business associate agreements in place. If Customer believes there has been unauthorized access to its Customer Account or Customer Data, Customer must immediately notify legal@commvault.com. In addition, Customer shall indemnify, defend and hold Commvault harmless from and against any damages and costs arising from or relating to Customer's failure to implement appropriate privacy and security safeguards to protect its Customer Account and Customer Data.

4. **Term and Termination.** This BAA is coterminous with the Terms and any applicable purchase order. Upon either party's knowledge of a breach or violation of this BAA by the other party, the non-breaching party will require the breaching party to take reasonable steps to cure the breach or end the violation. If the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party, or if no cure or end of violation is possible, the non-breaching party may terminate this BAA upon written notice to the breaching party in accordance with the Federal Acquisition Regulation and the Contract Disputes Act. If the Secretary provides guidance, clarification or interpretation of HIPAA or there is a change in HIPAA that the relationship between Commvault and Customer is not considered a Business Associate relationship, this BAA shall terminate and be null and void. Following expiration, cancellation or termination of the Terms and any applicable purchase order, Commvault and its subcontractors will destroy or return upon request all Customer Data which may include PHI within a reasonable amount of time unless such destruction or return is not commercially practical. Commvault shall continue to treat PHI as set forth herein for the duration of its possession thereof.

5. **Miscellaneous.** A reference in this BAA to a section in HIPAA means the section as in effect or as amended. Any ambiguity in this BAA shall be interpreted to permit compliance with HIPAA. The parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for compliance with the requirements of HIPAA. Except as expressly provided for in the Privacy Rule, there are no third-party beneficiaries to this BAA and Commvault's obligations are to Customer only. This BAA shall be governed by and construed in accordance with the Federal law of the United States as it pertains to the subject matter.

CUSTOMER NAME

_____

Name:
Email:
Date:

COMMVAULT

Name: Meg Cavanaugh
Title: Associate General Counsel

Commvault Master Terms & Conditions

Commvault's industry-leading Intelligent Data Services Platform empowers businesses to store, protect, optimize, and use data, wherever it lives. Delivering the ultimate in simplicity and flexibility, the Intelligent Data Services Platform is available as a license, term-based subscription, integrated appliance, or software-as-a-service.

1. **Solutions.** These Master Terms and Conditions (the "Terms") apply to Customer's use of Commvault's software or software-as-a-service (together, the "Solutions)."

   (a) **Software**. These terms apply to Commvault's on-premise software ("Software)."

   (b) **Software-as-a-Service**. These terms apply to Commvault's Metallic "SaaS Solution."

2. **Customer Use**. Customer is responsible for ensuring that it maintains and operates the information technology infrastructure from which the Solutions copy, back up, maintain, and transfer Customer's data including databases, applications, files, software, computers, servers, network hardware, or any other device (collectively, the "Customer Environment") and determining whether the Solutions meet Customer's technical, business or regulatory requirements. Commvault will cooperate with Customer's efforts to determine whether use of the Solutions is consistent with those requirements. Customer's shall not: (i) interfere with the proper working of the Solutions or, if applicable, impose an unreasonably large load on Commvault's infrastructure; (ii) copy, modify, disassemble, decompile or reverse engineer any part of the Solutions or apply any other process or procedure to derive source code or functionality of any software included in the Solutions; (iii) violate or infringe upon any third-party right, including any intellectual property right or right of privacy; (iv) initiate a denial of service attack, software viruses or other harmful or deleterious computer code, files or programs; (v) use the Solutions in order to build a similar or competitive application or service; or (vi) violate any applicable laws.

3. **Intellectual Property**. Commvault delivers great value to its Customers through its intellectual property. Customer agrees that Commvault-owned or licensed hardware, software, code, trademarks, trade secrets, proprietary methods and systems used to provide the Solutions (collectively, the "Commvault Technology") and the content made available or displayed by Commvault through the Solutions, including all text, graphics, images, trade names, service marks, product names, and the look and feel of the Solutions (collectively, the "Commvault Content") are owned by or licensed to Commvault. Other than the authorizations or licenses expressly granted by Commvault to Customer in these Terms, no assignment or other transfer of ownership shall be conferred or vest in and to the Commvault Technology or the Commvault Content to Customer, either by implication, estoppel, or otherwise.

4. **Professional Services**. Commvault may provide "Professional Services" which may be further described in a separate document. Customer acknowledges that all right, title and interest to any and all work or work products developed or produced during the performance of Professional Services are the sole property of Commvault. "Work or work product" means all ideas, concepts, know-how, techniques, inventions, discoveries, improvements, secret processes, trade secrets, trademarks, patentable, copyrightable subject matter or any other work developed or produced during the performance of the Professional Services, whether individually by Commvault or jointly with Customer. Customer is solely responsible for the protection of its legacy data during any Professional Services engagement. Commvault shall, at its own expense, purchase and maintain insurance for the duration of any Professional Services engagement. To the extent permitted by law and except for general employment solicitation practices, Customer agrees that it will not solicit for employment, or employ directly or indirectly, any employee of Commvault involved in a Professional Services engagement during such engagement, or for a period of twelve (12) months thereafter, without Commvault's consent. Customer acknowledges that the Professional Services will not customize or alter the value or functionality of any Software and no development activity will be included as part of Professional Services. Acceptance of any Software is not contingent upon the performance of the Professional Services.

5. **Free Solutions**. Commvault may provide Customers with a thirty (30)-day free trial or evaluation of the Solutions for non-production purposes (a "Trial"). Commvault may deactivate the Trial upon written notice. The Trial and related Solutions are provided "as is" and without representation, warranty, liability or indemnification obligations. Commvault is under no obligation to retain Customer data during a Trial. Customer will uninstall and destroy or return any Solution upon expiration of a Trial.

6. **Diagnostics & Feedback**. Commvault may collect or receive: (i) technical data, such as logs, reports and error messages, (ii) limited personal data, such as names and business contact details, (iii) reports and surveys regarding Customer's use of the Solutions which may include geolocation data ("Reporting"), and (iv) network architecture or security threat data (collectively, "Diagnostic Data") through the Solutions. Reporting may be disabled by Customer at any time via the dashboard. Further, Customer may provide Commvault with reports, comments, suggestions or ideas relating to the Solutions ("Feedback"). Customer agrees Commvault is free to disclose and use any Feedback, and derivatives thereto, and Customer does not obtain any intellectual property or any other right, title or interest in or to any aspects of the Solutions. Customer grants Commvault a worldwide, non-exclusive, royalty-free, fully-paid up, transferable and sublicensable right to use, reproduce, and modify Diagnostic Data in an anonymized manner.

7. **Confidentiality**. By the nature of Commvault's services, Commvault and its Customers regularly share confidential, proprietary information with each other. "Confidential Information" means any and all information and material disclosed by one party (the "Discloser") to the other party (the "Recipient") including but not limited to Customer Data, trade secrets, know-how, inventions, techniques, processes, programs, ideas, algorithms, formulas, schematics, testing procedures, software design and architecture, computer code, internal documentation, design and functional specifications, product requirements, problem reports, performance information, documents, and other technical, business, product, marketing, customer, financial information, or any other information the Recipient knows or ought to is confidential due to its nature. Recipient shall hold all Confidential Information in strict confidence and take the same degree of care that it uses to protect its own confidential information (but in no event less than reasonable care) to protect the confidentiality thereof. Confidential Information does not include information that (i) is or becomes generally known by the public, (ii) was or becomes available to a party on a non-confidential basis from a person not otherwise bound by the Terms of Service or is not otherwise known to be prohibited from transmitting the information, or (iii) is independently developed by the parties, provided that the party claiming an exception shall have the burden of establishing such exception. Commvault recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by Commvault .

8. **Termination**. Commvault may, upon reasonably practicable and lawfully permitted notice, temporarily suspend Customer's access to the Solutions or Professional Services, in whole or in part, for the following reasons: (i) a significant threat to the security or integrity of the Solutions, including if Customer's registration information is inaccurate or incomplete, or if Customer fails to maintain the security of its access credentials; (ii)reserved; or (iii)reserved When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, CommVault shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Commvault will use reasonable efforts to reestablish Customer's access to the Solutions promptly after Commvault determines that the issue causing the suspension has been resolved. Any suspension under this section shall not excuse Customer's obligation to make payments under these Terms. Either party may terminate these Terms immediately if the other party materially breaches its obligations hereunder, and such breach remains uncured for thirty (30) days following written notice to the breaching party.

9. **Effect of Termination**. Customer is responsible for preserving its data upon termination or expiration of these Terms. In the event of termination or

expiration of these Terms: (i) all rights and licenses to the Solutions and related materials shall immediately cease; (ii) Customer shall promptly pay Commvault any fees due and payable through the date of termination; (iii) Customer shall uninstall and destroy or return the applicable Solution, and (iv) Commvault may delete any Customer data Commvault has access to sixty (60)days following such termination or expiration. Customer's who require a long data retention period post termination or expiration must notify Commvault before the expiration of such sixty (60) day period and pay the then-current fees to preserve Customer data.

10. **Commvault Warranty**. Commvault warrants that the Solutions, Professional Services, support and maintenance shall be provisioned and performed in a diligent, prompt and professional manner by personnel with the requisite knowledge, skills expertise and training. Any Professional Services that are not of a professional quality shall be corrected by Commvault without charge, provided Customer gives Commvault written notice within fifteen (15) days upon completion. Commvault shall have a reasonable period of time, based on the severity and complexity of the defect, to correct the Professional Services. Commvault shall not be obligated to correct Professional Services if such defect is the result of Customer's actions or omissions. If Commvault is unable to correct the defect to Customer's reasonable satisfaction, Customer shall have no obligation to pay for the defective Professional Services. Commvault further warrants that it will comply with applicable law and the Solutions do not knowingly infringe upon any third-party's intellectual property rights. Except as otherwise stated in any product-specific terms, the Solutions are provided "as is" without representation or warranty, whether express, implied or statutory. Commvault specifically disclaims any implied warranties of merchantability, fitness for a particular purpose, non-infringement, title and quiet enjoyment or from a course of dealing, course of performance or usage in trade. Commvault and its licensors do not warrant that the Solutions will run properly in all IT environments, be uninterrupted or error-free, meet Customer's needs or requirements, or guarantee compliance with specific law.

11. **Limitation of Liability, Indemnification and Remedies**.

11.1 **Commvault Intellectual Property Indemnification**. Commvault is proud of the Solutions it builds and takes seriously the protection of our Customers' intellectual property and data. Commvault will indemnify, defend and hold Customer harmless against third-party claims that Commvault's proprietary technology or intellectual property within the Solutions infringes any validly issued patent, trademark or copyright, provided Customer shall give Commvault prompt, written notice of any such claim and Commvault shall have the authority to control the defense and settlement of the claim with counsel of its choice. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. Notwithstanding the foregoing, Commvault shall have no liability for any claim arising from: (i) any modification to the Solutions other than by Commvault; (ii) use of an outdated or discontinued versions of the Solutions;
(iii) use of the Solutions in combination with any products or services not provided or authorized by Commvault; (iv) use of the Solutions in violation of these Terms; (v) Commvault's compliance with Customer's designs, specifications, or instructions; or (vi) any claim for which Customer is obligated to indemnify Commvault. In the event the Solutions or any portion, becomes, or, in Commvault's opinion, is likely to become, subject to a claim of infringement of a third-party's intellectual property rights, Commvault may, in its sole discretion: (i) procure for Customer the right to continue use of the Solutions; (ii) replace or modify the Solutions with a version that does not infringe; or (iii) if Commvault cannot accomplish (i) or (ii) using commercially reasonable efforts, terminate these Terms and the applicable ordering documents.

11.2 **Commvault Data Privacy and Security Indemnification**. We exist in an ever-evolving data security threat landscape. Just as our Customers work diligently to protect against data security threats, Commvault is continuously advancing its privacy and security program, posture and vigilance to protect Customers' data. The Solutions may access and transfer information over the internet, and Commvault does not operate or control the internet. Viruses, worms, trojan horses and other undesirable data or components or unauthorized users (e.g., hackers) may attempt to obtain access to and damage Customer data, devices and networks. Commvault is not responsible for any such activities. Commvault will indemnify, have the right to intervene to defend and hold Customer harmless against third- party claims arising out of, or related to, any unauthorized, third-party access that results in compromise of unencrypted Customer data backed up by the Solutions to the extent such access or compromise was caused by Commvault, provided Customer shall give Commvault prompt written notice of such claim and Commvault shall have the authority to control the defense of the claim by counsel of its choice. In the event Customer seeks indemnification from Commvault pursuant to this provision, Customer's remedies shall be limited to actual and direct damages, excluding fines. This indemnification is conditioned on Customer partnering with Commvault during any investigation of potential or actual data compromises or breaches, including remediation efforts.

11.3 **Reserved**.

11.4 **Limitation**. Except as otherwise provided for herein or by applicable law, the aggregate liability of each party for all claims under these Terms is limited to direct damages up to one and one half of the amount paid for the Solutions or Professional Services during the twelve (12) months before the cause of action arose; provided, that in no event will a party's aggregate liability exceed the amount paid for the Solutions during the Term.

11.5 **No Special or Punitive Damages**. Neither party will be liable for loss of revenue or indirect, special, incidental, consequential, punitive, or exemplary damages, or damages for lost profits, revenues, business interruption, or loss of business information, even if the party knew they were possible or reasonably foreseeable. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor's gross negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

12. **General Provisions.**

12.1 **Export Controls and Trade Sanctions Compliance**. Customer's use of the Solutions is subject to compliance with U.S. and other applicable export control and trade sanctions laws, rules and regulations, including without limitation, the U.S. Export Administration Regulations, administered by the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") and U.S. trade sanctions, administered by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") (collectively, "Export Control Laws"). Customer acknowledges that the Solutions may not be available in all jurisdictions and that Customer is solely responsible for complying with applicable Export Control Laws related to the manner in which Customer chooses to use the Solutions, including Customer's transfer and processing of its data (if applicable) and the region in which any of the foregoing occur.

12.2 **U.S. Government End User Provisions.** Commvault provides the Solutions to federal government end users. Government technical data and software rights related to the Solutions include only those rights customarily provided to the public as defined in these Terms. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data), FAR 12.212 (Software), and FAR 52.227-14 (Rights in Data) and, for Department of Defense transactions, DFAR 252.227-7013 (Technical Data – Commercial Items).

12.3 **Data Privacy**. Customer does not transfer data to the EU and therefore is not subject to: (i) GDPR, or (ii) other applicable data protection laws requiring that processing be governed by a contract, therefore Commvault's Data Agreements is not applicable; however, (iii) HIPAA may be applicable and Customer agrees to the Business Associate Agreement, as amended,.

12.4 **Third-Party Products & Services.** Commvault may use third parties to assist in the provision of the Solutions and such third parties are intended beneficiaries of these Terms. As such, the Solutions may include third-party software, applications, platforms, messaging or communication services or API's, such as Microsoft Azure Cloud Computing Services, (collectively, the "Third-Party Services"). These Third-Party Services are not offered, controlled or provided by Commvault, and may be changed, modified or discontinued by the third-party without notice. Commvault expressly disclaims any and all liability related to, or arising from, the Third-Party Services, including Customer's use thereof, or any updates, modifications, outages, delivery failures, corruptions, discontinuance or termination of services by the Third-Party Service. Commvault is not responsible or liable for the manner in which Third-Party Services transmits, accesses, processes, stores, uses or provides data to Commvault. For a list of open source and third party licensing notices, please navigate here.

12.5 **Publicity.** Customer grants Commvault the limited right to use its company name as a reference for marketing and promotional purposes on Commvault's website and in other public and private communications extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. If Customer does not wish to grant these limited rights, Customer may opt-out by emailing customerchampions@commvault.com.

12.6 **Modifications.** Commvault may, from time to time, upgrade, update, or discontinue the Solutions, or portions or versions thereof, to provide ongoing innovation in the form of new services, features and functionality. In the event that Commvault discontinues a Solution or material portions or versions thereof that Customer has contracted for, Customer shall be entitled to a materially equivalent substitute or pro rata refund for any fees paid not used. Upon Commvault's notification, Customer may be responsible for installation of certain upgrades or updates. In the event of any material modifications, Commvault will notify Customer of such change by emailing the e-mail address Customer provides to Commvault or sending a message through Commvault's platforms.

12.7 **Assignment.** Neither party may assign these Terms, in whole or in part, without the other party's prior written consent,. Any attempt to assign these Terms other than as permitted herein will be null and void. Customer's right to use the Solutions, including any allotment of storage capacity or end users, shall not extend to acquired entities, in whole or in part, or new entities established as a result of an acquisition. In such event, the fees set forth in the order form shall be adjusted. Without limiting the foregoing, these Terms will inure to the benefit of and bind the parties' respective successors and permitted assigns.

12.8 **Audits.** Commvault may, upon forty-five (45) days notice and no more than once every twelve (12) months, audit Customer's installation and use of the Solutions to ensure Customer is in compliance with these Term and the applicable order form. Any such audit shall not unreasonably interfere with Customer's normal business operations. Customer agrees to cooperate with Commvault's audit and to provide reasonable assistance and access to information reasonably requested by Commvault. The performance of the audit and any non-public Customer data obtained during the audit (including findings or reports that result from the audit) shall be considered confidential information. If the audit identifies non-compliance, Customer agrees to remedy such non-compliance within thirty (30) days of written notification of that non-compliance (which may include, without limitation, the payment of any fees for additional Solutions). Customer agrees that Commvault shall not be responsible for any of Customer's costs incurred in cooperating with the audit.

12.9 **Force Majeure.** Excusable delays shall be governed by FAR 552.212-4(f).

12.10 **Governing Law and Language.** Without regard to conflict of law principles, these Terms will be governed by and construed in accordance with the Federal laws of the United States. Customer and Commvault agree not to participate in, or seek to recover monetary or equitable relief, in any lawsuit filed alleging class, collective or representative claims on a party's behalf. Customer acknowledges that any translation of the English language version of these Terms or any portion thereof is for convenience only, and the English language version will take precedence over the translation in the event of any conflicts arising from translation. Some jurisdictions restrict limitations of warranties or liabilities. Therefore, certain limitations herein may not apply to Customer.

12.11 **Notices.** Customer acknowledges that Commvault shall communicate with Customer electronically via its platforms or using the e-mail address provided by Customer. For contractual purposes, Customer consents to receive communications from Commvault in an electronic form and agrees this satisfies any legal requirement of notice delivery. Customer agrees that all notices are considered received by Customer within twenty-four (24) hours of the time posted to Commvault's website or platform, or the time emailed to Customer. Legal notices to Commvault shall be sent to contracts@commvault.com.

12.12 **Other Provisions.** These Terms, Commvault's Privacy Policy attached hereto, and the applicable order forms are an agreement between Customer on behalf of its affiliates and subsidiaries, as identified in the applicable order forms or as an end user of the Solutions, and Commvault Systems, Inc., including its affiliates and subsidiaries. Each party represents and warrants they have the authority to enter into this agreement and doing so does not conflict with any other agreement to which they are a party. In the event of a conflict between these Terms and the applicable ordering documents, any other document set forth by Customer or any previous agreement, these Terms shall prevail. Any preprinted terms in a purchase order are of no force and effect. The parties are independent contractors and will have no authority to assume or create any obligation or responsibility on behalf of each other. If any provision of these Terms is invalid or unenforceable under applicable law, then such terms will be changed, interpreted or severed, as appropriate to accomplish the objectives of such provision to the greatest extent possible under applicable law in order to protect the drafter, and the remaining provisions continue in full force and effect. No waiver of any term herein shall be deemed a further or continuing waiver. The sections of these Terms that ought to survive due to their nature shall survive any termination or expiration of these Terms and remain in full force and effect.

CUSTOMER

_____

Name:
Title:
Date:

COMMVAULT, SERVICES, INC.

_____

Name:
Title:
Date:

SAAS SOLUTION TERMS & CONDITIONS

Metallic's SaaS Solution is the "easy button" for cost-effective, secure and scalable data management, backup and security, with a single command center, enabling organizations to deliver on data protection strategies. Built with layered, air-gapped cloud security, secure and restrictive account access and data isolation, Metallic's SaaS Solution provides ease you can trust.

1. **Getting Started**. As a Customer you will register a Commvault account and provide Commvault with accurate and complete information (the "Customer Account"). Customers may authorize one or more of its employees, consultants, vendors or agents (collectively, "Authorized Users") to access and use the SaaS Solution on Customer's behalf. Each Authorized User will establish or be provided a username and password, and may also establish or be provided other access credentials, such as an encryption key (the "Access Credentials"). Customer acknowledges that its Authorized Users have full access to and management privileges of its Customer Account(s) and Customer Data. The term "Customer" is intended to include its Authorized Users for the purposes of the Terms.

2. **SaaS Solution Agent**. Customers may be required to download or install a software agent to support the SaaS Solution. Commvault grants Customers a limited, non-exclusive, non-sublicensable, non-transferable and revocable license to install, execute and use the agent solely in binary code form during the SaaS Solution Term, and access the SaaS Solution in accordance with the Privacy Policy, FAQs, website, user manuals and other information provided to assist Customer in its use and operation of the SaaS Solution (the "Documentation"). Customer's license to the agent is co-terminus with Customer's right to access and use the SaaS Solution for which the agent is required. Customer grants Commvault a worldwide, non-exclusive, royalty-free, fully-paid up, transferable and sublicensable right to use, replicate, deduplicate, and store Customer Data for the purpose of delivering the SaaS Solution pursuant to these Terms, improving the SaaS Solution, and as otherwise provided in Commvault's Privacy Policy. "Customer Data" means the data transmitted by Customer to Commvault in connection with the provision of the SaaS Solution.

3. **Global Availability and Support**.

3.1 Global Service and Support. Commvault is proud to administer the SaaS Solution from global geographic locations that best suit our Customers' needs. Where applicable and subject to data center availability, Customer Data will be backed up to a data center located in Customer's country of origin, or in a geographic location selected by Customer. For additional information, refer to the SaaS Solution configuration portal. Commvault is pleased to provide Customers with the support program for the SaaS Solution as set forth at Metallic Support. The support terms are incorporated by reference and may be modified from time to time in Commvault's sole discretion. Communications related to support of the SaaS Solution may be sent to customersuccess@metallic.io.

3.2 Global Availability. The SaaS Solution is available at least 99.9% of the time measured on a monthly basis ("Uptime"). The Uptime does not apply to any downtime due to: (i) any emergency or planned maintenance, repair, or upgrade; (ii) issues or failures with Customer's or its service providers' services, applications, software, hardware or other components not supplied by Commvault; (iii) third-party attacks, intrusions, distributed denial of service attacks or force majeure events, including those at Customer's site or between Customer's site and data centers made available through the SaaS Solution; or (iv) Customer's acts or omissions in violation of these Terms. In the event of Commvault's Uptime failure, Commvault shall: (i) use commercially reasonable efforts to provide Customer with an error correction or work-around that corrects the Uptime failure; and (ii) provide Customer with a credit as set forth in the table below (a "Service Credit"), provided such Service Credit is approved by Commvault, such approval not to be unreasonably withheld. For the avoidance of doubt, service providers are not eligible for Service Credits. Within thirty (30) days of the downtime incident, Customer must submit a Service Credit claim to Commvault with all information necessary for Commvault to validate such claim, including: (i) a detailed description of the incident; (ii) information regarding the time and duration of the downtime; and (iii) a description of the attempts to resolve the incident. Service Credits will be applied to Customer's next invoice. Customer is not eligible for any Service Credits if Customer's use of the SaaS Solution is free of charge. This is Customer's sole and exclusive remedy for any Uptime failure.

SaaS Solution Availability	Service Credit
Less than 99.9%	10%
Less than 99%	25%

3.3 Hosted Services. To the extent Customer uses Commvault's hosted storage, Customer acknowledges that such hosted storage is provided by Microsoft Azure Cloud Computing Services or, for U.S. federal government customers, Microsoft Azure for US Government. Customer's use of hosted storage services is subject to the then-current Microsoft Online Subscription Agreement(s) available at the following links: Azure and Azure for US Government. To the extent Customer uses its own hosted storage provider, the terms of such hosted storage provider shall govern. Customer is solely responsible for retention policies and any other policy settings, schedules, and configurable parameters applied to Customer Data, including implementing its own specific retention policies.

4. **Data Privacy & Security.**

4.1 Commvault Privacy and Security Program. Customer data privacy and security is Commvault's priority. Commvault represents and warrants that it maintains: (i) network security, business continuity and disaster recovery policies and procedures commensurate with industry best practices; and (ii) administrative, physical and technical safeguards designed to secure Customer Data from accidental or unauthorized access, use, alteration or disclosure. Commvault's collection, use, processing, storage and disclosure of any personal data included in Customer Data shall be in accordance with applicable data protection laws and Commvault's Privacy Policy. Customer acknowledges that it is Customer's responsibility to verify that the SaaS Solution' security and privacy protections are adequate and in compliance with all applicable laws governing the type of data included in Customer Data. Customer acknowledges (i) effective security is dependent on multi-layered, multi-faceted combination of solutions, deployed and managed in accordance with appropriate policies and procedures consistently applied, (ii) the quality of data, other output and strength of Customer's threat detection program are dependent on the configuration and deployment of the deceptive environment by Customer and its Authorized Users, and (iii) no individual element alone is sufficient to detect and prevent all security threats, as a result Commvault does not warrant and disclaims liability that all security threats will be detected and prevented by the Solutions. Customer agrees to, and will ensure that each Authorized User will, notify Commvault at ITCompliance@commvault.com immediately upon learning of any suspicious access to its Customer Account. Commvault's comprehensive privacy and security program is set forth in the Security Terms and incorporated herein by reference.

4.2 Access. Customer data privacy and security is Commvault's priority. At times, Commvault may be required to access or disclose Customer Data: (i) to provision the SaaS Solution to Customer pursuant to these Terms; (ii) to respond to a validly issued subpoena, an investigative demand or warrant; (iii) to investigate or prevent security threats, fraud, or other illegal, malicious, or inappropriate activity; (iv) to enforce or protect Commvault's rights and properties or those of its affiliates or subsidiaries; or (v) with the informed consent of the data subject. In the event Commvault is required to access Customer Data, Commvault shall not disclose Customer Data to third parties without Customer's consent or instruction, unless prohibited by law.

5. **Term**. Commvault initiates activation of the SaaS Solution upon receipt of a valid purchase order, by providing Customer with access to an account (the "Activation Date"). The term of Customer's subscription to the SaaS Solution shall begin on the Activation Date and continue as set forth on the applicable purchase order (the "SaaS Solution Term"). The SaaS Solution Term shall renew for an equal term unless either party provides written notice of non-renewal sixty (60) days prior to the renewal date.

6. **Customer Acknowledgments**. Customer agrees: (i) Customer and its

Authorized Users will keep Access Credentials confidential, and Customer remains responsible for the acts and omissions of its Authorized Users and any activity that occurs under its Customer Account(s) using the Access Credentials; (ii) Customer will use the most current version of the SaaS Solution at all times, unless otherwise agreed in writing; (iii) Customer is responsible for the security of its Customer Data if Customer disables any encryption or other security feature within the SaaS Solution; and (iv) Customer is responsible for maintaining its own internet and data connections, and components of the SaaS Solution that are accessed or used through internet connections and may be subject to Customers' internet service providers fees and downtime. Customer acknowledges Customer Data may not be available if: (i) Customer's initial backup and replication is not properly completed by Customer; (ii) Customer deletes Customer Data and does not restore it after deletion pursuant to Customer's data retention policies; (iii) Customer selects incorrect or inappropriate retention policies within the SaaS Solution; (iv) Customer's IT environment is unable to secure a connection with Commvault's servers or network; or (v) Customer fails to follow Commvault's technical requirements and the Documentation for utilizing the SaaS Solution, including installing updates, or failing to periodically test Customer's backups and restores, or ensure that Customer Data is protected and not otherwise corrupted.

Commvault Software Terms & Conditions

Commvault's Software delivers a unified solution combining backup and recovery with disaster recovery to deliver enterprise-grade data protection that is powerful and easy to use and provides data availability and business continuity across on-premise and cloud environments using a single extensible platform.

1. **Getting Started**. Commvault grants Customer a limited, non-exclusive, non-sublicensable, and non-transferable license to install, execute and use the Software (including Software embedded in any hardware, if applicable) solely in binary code form during the Software Term (defined below), in accordance with the applicable ordering documents, Commvault's Privacy Policy, FAQs, website, user manuals and other information provided to assist Customer in its use and operation of the Software (collectively, the "Documentation"). The Software is licensed, not sold and except as set forth herein, all sales of Software are final, non-returnable and non-refundable. Acceptance of the Software occurs upon delivery. Software license key(s) are electronically delivered by Commvault. Any Software license acquired by virtue of Customer's use or purchase of hardware shall be limited to the hardware upon which the Software was originally installed. Customer may be required to periodically reapply Software license keys during the Software Term which Commvault shall provide. Customer may make a copy of the Software solely for back-up purposes, provided such back-up copy is used only as a replacement for the original copy on the same hardware upon which the Software was originally installed. Customer may use the Software solely for its internal data center operations.

2. **Capacity**. Customer shall activate and maintain the reporting features of any capacity-based Software and provide usage reports to Commvault upon request. In the event Customer's use of limited capacity-based Software exceeds capacity, Customer shall be obligated to pay Commvault, directly or through its authorized reseller, for all excess usage. Software purchased on a capacity-basis may cease to operate and perform if Customer exceeds capacity. If Customer purchases unlimited capacity Software for itself and/or its affiliates and subsidiaries: (i) the Software may be used by Customer's affiliates and subsidiaries in the territory set forth in the order forms only, (ii) Customer assumes all liability for those affiliates and subsidiaries, and (iii) upon acquisition of Customer's business by another entity, the unlimited capacity Software license shall terminate, and Customer will retain a limited license for the Software then-deployed in Customer's environment for the remainder of the Software Term.

3. **Maintenance & Support**. Commvault provides support and maintenance for the Software as set forth here at Commvault's then-current pricing. Customers who purchase support and maintenance must do so for all Software in Customer's Environment. Maintenance and support commence upon delivery of the Software, if applicable.

4. **Commvault Software Warranty**. Commvault warrants that the Software shall substantially perform in accordance with the user documentation for a period of ninety (90) days from the date of delivery (the "Warranty Period"). During the Warranty Period, if the Software is defective, Customer must immediately notify Commvault in writing, and Commvault, in its discretion, will either: (i) repair or replacement the defective Software; or (ii) return prorated fees paid by Customer for the defective Software, in which case Customer shall uninstall and return or destroy the defective Software.

5. **Term**. The term of Customer's license to the Software shall begin on the date the Software is delivered and continue as set forth in the applicable order form (the "Software Term"), except where such license is perpetual. The Software Term may renew for an equal term by executing a written order for the renewal terme. Upon expiration of the Software Term, Customer may use a limited recovery version of the Software solely for recovering data backed up by the Software during the Software Term.

Commvault Privacy Policy

Effective Date: June 8th, 2021

Commvault Systems, Inc. and all its entities, subsidiaries, branches, representative offices, affiliates and other Commvault group companies ("**Commvault**" or "**we**") respect your privacy.

This Privacy Policy provides information for our customers, partners, suppliers and other individuals and organisations that we may have a business relationship with about how we collect, use and share personal information.

Data Controller

Commvault Systems, Inc. is headquartered in Tinton Falls, New Jersey, United States but we have offices around the world. To comply with applicable data protection laws, Commvault has implemented a global data protection program based on requirements set forth by the EU General Data Protection Regulation 2016/679 ("**GDPR**"). Where required, we comply with other applicable data protection laws.

With regards to the General Data Protection Regulation and other applicable data protection laws the Commvault entity that is the data controller of your personal data will depend on the situation in which the data has been collected.

The EU representative and the main establishment for all our EU affiliates for purposes of compliance with the GDPR is:

Commvault Systems International BV

Papendorpseweg 75-79, 3528 BJ Utrecht, Netherlands

The personal data that we collect and our basis for processing

Personal data is any information that can be used to directly or indirectly identify an individual, and may include your name, address, email address, phone number, contact preferences, electronic identifiers, IP address and other.

Commvault will use your personal data based on:

- **Our legitimate business interests**: For example, in connection with direct marketing or service improvement. Where we rely on this basis, we carry out a legitimate business assessment to ensure that our business interests do not override your rights. In some cases, you may have the right to object to this use of your personal information. For more information please read the 'Your Rights' section of this Privacy Policy.
- **Contract**: Where it is necessary in connection with a product or service, we are providing to you. For example, we may process personal information to establish a contract for goods or services between you and Commvault, or to send you invoices for ordered goods or services.
- **Legal obligation**: Where it is reasonably necessary for compliance with a legal obligation to which we are subject to e.g. tax laws, export control compliance or to exercise or defend the legal rights.
- **Consent**: If we are not relying on another basis for processing your personal information, we will seek your consent prior to any use of your personal data. A clear request for your consent will be presented to you and you will have the ability to withdraw your consent at any time.

Except for certain information that is required by law or by Commvault's policies, your decision to provide any personal data to us is voluntary. You will therefore not be subject to adverse

consequences if you do not wish to provide us with your personal data. However, please note that if you do not provide certain information, we may not be able to accomplish some or all of the purposes outlined in this Privacy Policy, and you may not be able to use certain services or which require the use of such personal data.

We collect personal data of our employees, potential employees, clients, suppliers, business partners, shareholders, customers and product/service/website users. If the data we collect is not listed in this Privacy Policy, we will give individuals (when required by law) appropriate notice of which other data will be collected and how they will be used.

We may collect personal data directly from you (e.g. when you interact with us) or indirectly (e.g. from our business partners and/or commercially available third-party sources).

The personal data categories we collect can include the following:

- **Identification data**: name and business contact details (such as email address, mailing address, contact phone number, position, company)
- **Transaction data**: such as bank account credit or debit card details and related personal data necessary for us to make and receive payments
- **Your interactions with us**: other information you choose to provide, such as when you submit a recruitment application, inquiry or complaint, seek customer support, respond to a survey , enter a contest or promotion, contact our representatives or content of social media messages, posts, likes and responses to and about Commvault
- **Online behaviour and preferences data**: information collected via cookies and other tracking technologies such as IP address, device identifier, location data, browser type and language,

access times, other unique identifiers and other technical data that may uniquely identify your device, system or browser, as well as credentials such as your passwords, account history, password hints, and similar security information used for authentication;
- **Demographic information:** such as your age, gender, country, interests, and preferences, including preferences related to marketing and communications
- **Audio-visual data:** where applicable and legally permissible, we process CCTV footage of our office areas or recordings of phone or video calls or chats with us (e.g. during customer support interactions)

Our products and services are not directed at children.

How we use personal information

We may use your personal data to operate our business, provide our solutions and for other legitimate purposes permitted by law. Some of the ways we may use your information are illustrated below:

- To personalize the look and feel of our websites that you visit, to match personal preferences that we have inferred from your use of the website and to provide you with the appropriate local version of the website (see the "Cookies" section for more information). For example, we may use web log information, cookies or web beacons in ways that help us maintain some of your site preferences. You may choose whether or not to allow cookies or web beacons to track your browser preferences. To find out more about cookies, please read the Cookies section of this Privacy Policy.
- To communicate with you regarding our products and services;
- To provide, maintain and enhance our products and services;

- To fulfil a contract, or take steps linked to a contract, with you or your organisation;
- To provide you with technical support, troubleshooting or other similar services;
- To process payments, billing and collection;
- To manage customer and partner relations;
- To manage our suppliers;
- To sell and market our products and services including conducting marketing campaigns, to provide you with a newsletter subscription, to plan and host events, online forums or webinars;
- To provide customer support;
- To carry out business analytics. For example we may process information in the email header of business emails sent and received by us (including the names of recipient and sender, date and time of the email) for the purposes of evaluating our existing or prospective business relationship;
- To listen to a call recording for training, quality control or process improvement purposes;
- To manage access to our premises and for physical security purpose;
- To detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity;
- For internal purposes such as auditing, analysis, and research to improve our products or services;
- To comply with and enforce applicable legal requirements (e.g. maintaining records, tax law, immigration law, compliance checks, anti money laundering, trade sanctions, whistleblowing, complying with data subject requests etc.), relevant industry standards and Commvault's policies; and
- To recruit and manage employment relationship (for specific information regarding employment please refer to our Privacy Charter)

Providing information to others

We may need to share information about you:

- With other companies in the Commvault group, our partners, suppliers or agents who perform services on our behalf, such as processing of orders, providing customer support or providing advertising on the website;
- In response to a request for information from a competent authority if we believe disclosure is in accordance with, or is otherwise required by any applicable law, regulation or legal process with law enforcement bodies or other third parties as necessary to comply with the law, including to meet national security or law enforcement requirements;
- If we decide to re-organize or sell our global businesses we may need to disclose your personal information in the course of this activity to prospective purchasers; or
- If we otherwise notify you of the disclosure and you consent to it.

International data transfers

To offer you the best possible products and services and remain competitive in our business, we may transfer data across Commvault's affiliates in different geographies and locations. Countries may have different laws and data protection compliance requirements, with some providing more protection than others. Commvault will take appropriate steps to ensure your personal data is handled as described in this Privacy Policy. Where required, we comply with applicable legal frameworks relating to the transfer of personal data. For example we only make these transfers, where the EU has made an "adequacy decision" for the country to which the data will be transferred or where we have put in place the

“appropriate safeguards” that the law requires such as signing EU Standard Contractual Clauses.

Update: Following the invalidation of the Privacy Shield by the Court of Justice of European Union, Commvault has withdrawn from Privacy Shield. As of June, 8th 2021 Commvault does no longer participate in or comply with Privacy Shield. Following the withdrawal, Commvault shall however retain data collected and transferred under Privacy Shield and will continue to apply the Privacy Shield Principles to such data.

Keeping information secure

We employ information security specialists and invest significant resources on technical and operational security measures to help us protect your personal information from loss, misuse, unauthorised access, modification or disclosure. However, we cannot be held responsible for unauthorised or unintended access that is beyond our reasonable control.

Keeping your personal data

We keep records for as long as necessary to provide the relevant product or service, and in accordance with applicable legal, tax and accounting requirements. When your information is no longer required, we will ensure it is destroyed in a secure manner.

Cookies

Our websites use cookies (which includes third-party cookies to support analytics functionality) and other similar technologies to improve the user experience.

You can check and adjust your cookie preferences by clicking the link below.

Cookie Preferences

Your rights

Your local law may provide rights regarding the use of your personal data. Where the GDPR applies to personal data, it gives individuals resident in the EU certain rights that they can exercise free of charge. These include the:

- Right to correct your personal information
- Right to access your personal data
- Right to data portability
- Right to object to use of personal data (for example, where we are using it for direct marketing or our lawful basis is our legitimate interest)
- Right to restrict the use of your data in some circumstances
- Right to erasure in some circumstances

If you would like to assert one or more of these rights, please email or write to us at the address set out in the Contact section of the Privacy Policy. We will respond to your requests within applicable timeframes.

You may also unsubscribe from receiving our email marketing communications at any time by following the “unsubscribe” instructions included in our communication.

Complaints process

If you have a complaint about how we have handled your personal data, you may contact us directly using the details below or you can contact the applicable competent data protection authority.

Updates

We regularly review and update this Policy. If we make a change, we will post the updated version on our site.

Contact

If you have any questions about this Policy, or would like to exercise your rights with respect to your personal information, please contact our Global Data Governance Officer via GDGO@commvault.com via or write to:

For U.S. and all locations other than EEA, UK and Switzerland:

Commvault Systems, Inc.

Attn: Legal Department & Global Data Governance Officer

1 Commvault Way

Tinton Falls, New Jersey 07724, United States.

For EEA, United Kingdom, Switzerland:

Commvault Systems International BV

Attn: Legal Department & Global Data Governance Officer

Papendorpseweg 75-79, 3528 BJ Utrecht, Netherlands