FINANCIAL SERVICES ADDENDUM

NOT FOR EDITING OR NEGOTIATION
Version Date: January 10, 2025

This **Financial Services Addendum** ("**Addendum**") is entered into between Elastic and Customer and sets forth additional terms and conditions related to Customer's purchase of a Cloud Service or Software Subscription (as applicable). The "**Effective Date**" of the Addendum is the: (a) the date of the last signature on an Order Form between Customer and Elastic; (b) the date upon which Customer accepts a private offer via the applicable Marketplace; or (c) the date of the last signature on an Order Form executed by Elastic and a Reseller on behalf of Customer.

1. DEFINITIONS.

Capitalized terms shall have the meanings specified below. Capitalized terms not defined in this Addendum shall have the meanings set forth in the Agreement:

"**Agreement**" means collectively, the Subscription Agreement, this Addendum, any document incorporated by reference, and any applicable Order Form.

"**Applicable Law**" means the applicable laws and regulations administered by a Regulator in connection with Customer's access and use of a Cloud Service or Software Subscription, including, the EBA Guidelines, the EIOPA Guidelines, BRRD and DORA.

"**BRRD**" means the Directive 2014/59/EU establishing a framework for the recovery and resolution of credit institutions and investment firms and any national laws implemented by a member of the European Union.

"**Cloud Service**" means an Elastic software-as-a-service offering, that is generally made available by Elastic to its customers through either Amazon Web Services ("**AWS**"), Microsoft Azure ("**MSFT**") or Google Cloud Platform ("**GCP**") Infrastructure as a Service ("**IaaS**") which Elastic uses to provide a Cloud Service. For clarity, a Cloud Service does not include "Elastic Site Search" and "Elastic App Search".

"**Subscription Agreement**" means the terms and conditions applicable to Customer's access and use of a Cloud Service and/or Software Subscription as set forth in the applicable Order Form.

"**Customer**" means the Customer entity set forth in: (a) an Order Form between Customer and Elastic; (b) the private offer submitted by Elastic via the applicable Marketplace; or (c) an Order Form executed by Elastic and a Reseller on behalf of Customer.

"**DORA**" means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

"**EBA Guidelines**" means EBA/GL/2019/02, "Guidelines on Outsourcing Arrangements", published by the European Banking Authority on 25 February 2019.

"**EIOPA Guidelines**" means EIOPA-BoS-20-002, "Guidelines on Outsourcing to Cloud Service Providers", published by the European Insurance and Occupational Pensions Authority on 6 February 2020.

"**Elastic**" means the Elastic entity set forth in: (a) an Order Form between Customer and Elastic; (b) the private offer submitted by Elastic via the applicable Marketplace; or (c) an Order Form executed by Elastic and a Reseller on behalf of Customer.

"**Elastic Security Standards**" means Elastic's information security standards set forth in the Elastic Information Security Addendum located at https://www.elastic.co/pdf/elastic-information-security-addendum-consolidated-v030121-3.pdf, a copy of which is attached for reference in **Exhibit A**.

"**Order Form**" means an ordering document provided by Elastic pursuant to which Customer, or a Reseller acting on Customer's behalf, purchases a Cloud Service and/or Software Subscription.

"**Security Incident**" means an event that significantly compromises or degrades the security of the network and information systems of a Cloud Service, that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Content.

"**Software**" means Elastic's software that is licensed for use on Customer's premises or in Customer's public cloud account under a Subscription ("**Customer Location**"), including all updates and new releases that are generally made available by Elastic to its customers under the Agreement.

"**Regulator**" means a government or regulatory body, with binding authority over Customer's activities.

"**SLA**" means the Service Level Agreement attached in **Exhibit B**, which sets forth Elastic's service level terms and conditions, as well as provides a description of Elastic's service levels with respect to a Cloud Service.

"**Subcontracting**", means a situation where Elastic hires another service provider to provide a material part of a Cloud Service. The term "**Subcontractor**" shall be construed accordingly.

2. LOCATION.

Elastic uses Infrastructure as a Service (IaaS) providers, such as AWS, MSFT, and GCP to host and provide a Cloud Service. Elastic does not maintain any physical data centers. Elastic has provided Customer with a choice of data hosting regions for a Cloud Service ("**Hosting Region**") and Customer can elect at its sole discretion via the Cloud Service interface, to have a Cloud Service hosted within the territory of the European Union or elsewhere (including in the US or the APJ region). Customer may request the address of the applicable data center(s) with respect to its Hosting Region from Elastic. Elastic shall not further process Content from outside the Hosting Region except as necessary to provide Support Services requested by Customer in accordance with the Agreement, or as necessary to comply with the law or binding order of a governmental body. With respect to Software, Customer shall be solely responsible for installing and operating the Software from the Customer Location.

3. SERVICE LEVEL AGREEMENT.

For a Cloud Service Subscription for which Customer has implemented a high-availability (i.e. redundant) configuration, a Cloud Service shall meet or exceed the service level requirements set forth in the SLA. Customer may monitor Elastic's performance of a Cloud Service at https://status.elastic.co. To receive updates regarding the availability of a Cloud Service, Customer must subscribe via at the URL set forth above.

4. INFORMATION SECURITY PROGRAM.

4.1 **Information Security**. With respect to a Cloud Service, including Content, Elastic shall adopt and maintain up-to-date and robust security measures as set forth in the Elastic Security Standards and evidenced by Elastic's: (a) System Organization Controls 2, Type 2 report (for availability/security and confidentiality) ("**SOC 2 Report**"), which includes confirmation that Elastic maintains a Business Continuity Program (as defined in Section 5 below) for a Cloud Service, together with a description of the controls Elastic operates for its business continuity system plan; (b) certification under ISO 27001 ("**ISO 27001 Certification**"); or (c) in each case, such alternative industry standard reports or certifications that are its successor or reasonable alternative (provided that they are at least as protective as the standards set out above) as determined by Elastic. Elastic shall implement processes for regularly testing, assessing and evaluating the effectiveness of the Elastic Security Standards. At least annually, Elastic shall conduct a third party penetration testing against a Cloud Service, including evidence of data isolation among tenants in the multi tenant Cloud Service. Upon request, Elastic shall provide Customer with a summary report of the results of such penetration testing. For Software, the parties agree that as Software is installed in and operated from the Customer Location by Customer. Customer is solely responsible for implementing its own information security requirements.

4.2 **Software Updates**. In accordance with the Support Services Policy, Elastic shall provide necessary updates, patches, and upgrades to maintain the operational resilience of the Software and shall make available applicable Documentation located at https://www.elastic.co/docs to enable Customer to install and operate the Software at the Customer Location. Customer is solely responsible for ensuring the timely application of necessary updates, patches, and upgrades provided by Elastic to maintain the operational resilience of the Software.

5. BUSINESS CONTINUITY PROGRAM.

Elastic shall maintain a business continuity program during the applicable Subscription Term ("**Business Continuity Program**"), such that despite any disruption in Elastic's ability to perform its obligations under the Agreement from any particular location or through the efforts of any particular individuals, Elastic shall be able to continue to perform its obligations from an alternate location or with replacement personnel. Elastic shall test its Business Continuity Program and update it annually.

6. SECURITY INCIDENTS.

Upon becoming aware of a confirmed Security Incident, Elastic shall: (a) without undue delay, notify Customer at the Customer designated email address of the 'Organization Owner' associated with a Cloud Service, of the discovery of the confirmed Security Incident, which shall include a summary of the known circumstances of the Security Incident and the corrective actions taken or to be taken by Elastic; (b) conduct an investigation of the circumstances of the Security Incident; (c) use commercially reasonable efforts to mitigate the effects of the Security Incident; (d) use commercially reasonable efforts to communicate and cooperate with Customer concerning its responses to the Security Incident; and (e) cooperate with a Regulator, including persons appointed by such Regulator. Elastic's notification of or response to the Security Incident shall not be construed as an acknowledgement by Elastic of any fault or liability with respect to the Security Incident.

7. SUBCONTRACTING.

7.1 **Subcontractor List**. Customer authorizes the engagement of the Subcontractors listed at https://www.elastic.co/agreements/cloud_services/chain_subcontractors ("**Subcontractor List**"). A current copy of the Subcontractor List is attached in **Exhibit D**. Elastic has entered into a written agreement with each Subcontractor and has imposed obligations on each such Subcontractor, such as confidentiality, data protection, data security and business continuity. Elastic shall oversee the performance of each Subcontractor with respect to any applicable subcontracted services. Elastic shall remain fully liable for the performance of the Subcontractors. Elastic shall conduct regular due diligence on the Subcontractors (which includes reviewing industry standard reports and certifications), and reasonably assure itself, based on their responses, that such Subcontractors have in place security controls that are substantially similar to the Elastic Security Standards.

7.2 **Change to Subcontractors**. Elastic may update the Subcontractor List, in particular where this might affect the ability of Elastic to meet its responsibilities under the Agreement, by updating the Subcontractor List located at https://www.elastic.co/agreements/cloud_services/chain_subcontractors. Customer must subscribe to the RSS feeds available via at the URL set forth above. Any updates to the Subcontractor List shall take effect 120 days following the date of such update, unless the update is made to address an existing or imminent risk to a Cloud Service, in which case Elastic will provide Customer as much advance notice as is reasonably possible.

7.3 **Objections to a Change to Subcontractors**. Customer may object to any updates to the Subcontractor List by notifying Elastic in writing within the 120 days described above. Customer's notice shall explain the reasonable grounds for the objection. Elastic shall use reasonable efforts to make available to Customer a change in the Cloud Service or recommend a commercially reasonable change to Customer's configuration or use of a Cloud Service to resolve the objection raised by Customer. If such change or recommendation is not possible with reasonable commercial efforts within a period of 60 days from receipt of Customer's notification, and where Customer's continued use of the Cloud Service would result in undue Subcontracting, Customer may terminate in writing the applicable Cloud Service Subscription. If Customer does not object within such 120 days, it shall be deemed to have accepted the update to the Subcontractor List.

8. REPORTS AND CERTIFICATIONS/ RIGHT OF ACCESS AND AUDIT.

The parties agree that, except for providing the Customer with relevant information applicable to Software upon Customer's request, including any applicable security documentation to facilitate Customer's third-party risk assessments, the remaining provisions of this Section 8 shall not apply with respect to Software installed in and operated from the Customer Location.

8.1 **Copies of Reports and Certifications**. No more than once per calendar year during the applicable Subscription Term, and upon advance written request from Customer, Elastic shall make available to Customer at no additional charge; (a) copies of Elastic's SOC 2 Report or ISO 27001 Certification (for clarity, it shall not constitute a breach of the Agreement by Elastic, if exceptions are identified in any SOC 2 Report (or its successor or alternatives), provided that Elastic has taken appropriate steps, in its sole discretion, to remediate those exceptions); and (b) to the extent permitted by the applicable agreement between Elastic and its Subcontractor(s), make available to Customer any information, responses, and documentation provided by the applicable Subcontractor to Elastic concerning the information and security programs implemented by the Subcontractor with respect to the portions of a Cloud Service Subcontracted to such Subcontractor (together with the SOC 2 Report and the ISO the "**Certifications and Reports**"). Disclosure of certain Subcontractor information may require Customer to first agree to hold such information in confidence pursuant to a binding non-disclosure agreement between Customer and the applicable Subcontractor.

8.2 **Right of Access and Audit**. Where Customer has determined that the Certifications and Reports are insufficient for compliance with its then applicable regulatory obligations or, if Elastic has implemented a process for pooled audits in co-operation with other Elastic customer, Elastic agrees to provide Customer or the Regulator ("**Requester**"), at Customer's sole cost and expense, no more than once per calendar year during the applicable Term (unless otherwise required by a Regulator) and upon 30 days prior written notice, with access to Customer's Cloud Service deployment and to any applicable business premises (excluding the personal residences of Elastic personnel), personnel and data applicable to Customer's Cloud Service deployment, to enable the Requester to monitor Customer's Cloud Service deployment and ensure compliance with all applicable regulatory and contractual requirements ("**Right of Access and Audit**"). Any results and/or findings resulting from a Right of Access and Audit exercised by a Requestor ("**Audit Results**") shall be provided to Elastic within 7 days of completion of such Right of Access and Audit. Customer shall ensure that such Audit Results are not disclosed to any third party (except a Regulator, subject to Section 15 below or, if required by Applicable Law) without Elastic's prior written consent.

8.3 **Proportionality**. The Right of Access and Audit set forth in Section 8.2 above shall be exercised by a Requestor in a proportional manner, minimizing disruption and taking into account the complexity, risks, criticality, importance of a Cloud Service, using a risk-based approach and proportional manner, and adhere to relevant, commonly accepted, national and international audit standards, including Elastic's reasonable security and other site regulations for the premises at which the Right of Access and Audit activities are conducted. No less than 14 days prior to any agreed upon Right of Access and Audit, the Requester shall submit to Elastic a detailed Right of Access and Audit plan describing the scope and duration of the proposed Right of Access and Audit activity.

8.4 **Third Party Auditor**. At the Requestor's sole cost and expense, the Requester may appoint a reputable independent third party to exercise the Right of Access and Audit in accordance with this Section 8 ("**Third Party Auditor**") provided that such Third Party Auditor executes a mutually agreed upon Non-Disclosure Agreement. Such Third Party Auditor shall not be a direct competitor of Elastic or the applicable Subcontractor. Requester shall verify that its and any Third Party Auditor's personnel performing the Right of Access and Audit activity have acquired the right skills and knowledge to perform effective and relevant audits and assessments of the Customer's Cloud Service deployment. The Requester shall be solely responsible for any acts or omissions of its Third Party Auditor.

8.4 **Access to Content by a Regulator**. A Requester who is a Regulator, or a Third Party Auditor may require Elastic to provide the Regulator or Third Party Auditor with direct access to Customer's Content. Accordingly, Customer expressly authorizes Elastic to grant administrative rights to Customer's Account for its Cloud Service deployment to individuals designated by the Regulator or Third Party Auditor to enable such individuals to access Customer's Content. Customer remains solely responsible for any access to Customer's Content by a Regulator or Third Party Auditor.

8.5 **Exclusions**. A Requestor, including any Third Party Auditor shall not be allowed access to any deployments and/or data belonging to any other Elastic customer, including any privileged or attorney work product information of Elastic or its Affiliates, customers, Subcontractors, or third parties. If the exercise of the Right of Access and Audit could, in Elastic's reasonable opinion, create a risk for another Elastic customer's environment (including due to its impact on service levels, availability of data, and confidentiality), Elastic and the Requester will agree on an alternative way to address the request that provides Requester a similar level of assurance while ensuring that risks to another Elastic customer's environment are avoided or mitigated.

8.6 **Direct agreement between Subcontractor and Customer**. Notwithstanding the terms of this Addendum, in the event that Customer has entered into a direct financial services agreement with a Subcontractor, the rights and obligations provided for in that direct financial services agreement shall control as Customer's Right of Access and Audit and other Customer regulatory compliance requirements. Furthermore, Customer's Right of Access and Audit as it relates to MSFT as a Subcontractor is restricted by MSFT's to Microsoft's Online Services operations and controls. "Online Services" means, all Microsoft's Online Services referred to as "Core Online Services" as defined in the Online Services Privacy & Security Terms, currently available at https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all, and subject to SSAE 18 SOC 1 Type II and SSAE 18 SOC 2 Type II audits. A current list of the Core Online Services at the Effective Date of this Addendum is attached as **Exhibit C**.

9. SIGNIFICANT DEVELOPMENTS.

Elastic shall make the following available to Customer via the Cloud Service interface or the URL link set forth in Section 3 above: (a) information about developments that materially impact Elastic's ability to perform a Cloud Service in accordance with the SLAs ("**Significant Developments**"); and (b) if available, reports describing the cause of the applicable Significant Development and summarizing the actions taken by Elastic to resolve it. For clarity, information with respect to Significant Developments shall be deemed Elastic Confidential Information.

10. AWARENESS TRAINING.

Elastic shall ensure that all employees of Elastic who have access to Customer Information: (a) are subject to confidentiality obligations no less stringent than the confidentiality obligations set forth in the Agreement; (b) are suitably qualified and kept up to date on Elastic's security awareness programmes and digital operational resilience training, maintaining the required technical skills, and receiving and participating in the cybersecurity training provided by the Elastic at least once a year.

11. TERMINATION RIGHTS

In addition to any other termination rights set forth in the Agreement, Customer or Elastic (as applicable) may terminate the applicable Subscription as follows:

(a) where either party is in a material breach of Applicable Law, provided that, if the material breach in question is curable, the other party shall only be entitled to terminate the applicable Subscription if the breaching party has failed to cure such breach within 30 days following a request in writing from the other party to do so;

(b) where circumstances capable of altering the performance of a Cloud Service or Software are identified by Customer and notified to Elastic, provided that: (i) Customer can reasonably demonstrate that such circumstances have a material and adverse effect on a Cloud Service or Software; and (ii) such circumstances are not remedied by Elastic to the reasonable satisfaction of the Customer (acting in good faith) within a time that is reasonable given the circumstances concerned;

(c) where weaknesses regarding the management and security of a Cloud Service, Customer's Content, or Software are identified by Customer and notified to Elastic, provided that: (i) Customer can reasonably demonstrate that such weaknesses have a material and adverse effect on a Cloud Service, Customer's Content or Software; and (ii) such weaknesses are not remedied by Elastic to the reasonable satisfaction of the Customer (acting in good faith) within a time that is reasonable given the weaknesses concerned;

(d) upon 30 days prior written notice, where there is a material change notified to Customer affecting the Agreement or Elastic, and having in good faith considered the change, Customer is not satisfied (and can evidence the same to Elastic) that it will be able to comply with its obligations given the occurrence of such change;

(e) if Customer is instructed by a Regulator to terminate the Subscription or the Customer is informed by a Regulator, that, due to the condition or circumstances related to the Agreement, such Regulator is no longer in a position to effectively supervise the Customer, and the Regulator is not satisfied that any proposed arrangement (reasonably agreed between the parties) is capable remedying its inability;

(f) Elastic shall have the right to terminate the applicable Subscription with 30 days' notice in the event of a material change in a legal or regulatory requirement which, in Elastic´s reasonable opinion, makes it no longer economically viable to provide a Cloud Service and/or Software and the parties have been unable to agree any amendments to the Agreement to resolve the concerns; or

(g) either party may terminate the applicable Subscription, immediately, if the other party becomes the subject of a voluntary or involuntary petition in bankruptcy or any involuntary proceeding relating to insolvency, receivership, liquidation, or similar action for the benefit of creditors as a consequence of debt, or if the other party otherwise ceases or threatens to cease business.

12. BRRD REQUIREMENTS.

To the extent that Customer is subject to the requirements of the BRRD, and provided that Customer continues to fulfill its substantive obligations under the Agreement (in the meaning of Article 68 of the Directive 2014/59/EU), including its payment obligations, in the event that Customer is taken into resolution or early intervention or any other similar regulatory measure adopted by a Resolution Authority or Competent Authority (as both terms are defined in Article 2 of the BRRD), Elastic shall, if so requested in writing by Customer, cooperate in good faith with the Resolution Authority or Competent Authority regarding any concerns in respect of the ongoing provision of a Cloud Service or Software to Customer. Such cooperation shall be without prejudice to any rights or remedies Elastic has under the Agreement.

13. DELETION OF CONTENT.

During the applicable Subscription Term, Elastic shall provide Customer with access to, and the ability to download and/or delete, all Content. Customer acknowledges that it remains at all times solely responsible for deleting or retrieving Content from a Cloud Service prior to termination of the applicable Subscription and/or Customer's Account for any reason. In the event of the termination of the applicable Cloud Service Subscription, Elastic shall delete all Content from the applicable Cloud Service, using commercially reasonable efforts to do so within 45 days of such discontinuance, other than copies of Content: (a) required to be retained by applicable law; or (b) stored in Elastic's backups and disaster recovery systems, which in each case shall be deleted in the ordinary course in accordance with Elastic's data retention policies. Customer retains full control over Content it processes in a Cloud Service and has the right to delete any Content from a Cloud Service at any time during the term of the applicable Subscription Term.

14. EXIT MANAGEMENT.

In the event of a termination of the Subscription, Elastic shall, acting in good faith, provide Customer with reasonable assistance in order to enable Customer to transition to a new third party service provider ("**Transition Services**") subject to mutual agreement between the parties as to the nature of each party's obligations and, if applicable (and mutually agreed), appropriate fees for such Transition Services. Elastic warrants that any Transition Services provided by Elastic will be provided to maintain continuity of service (as mutually agreed between Elastic and Customer) and with minimal disruption to Customer's business during the Transition Services. Without prejudice to the foregoing, and upon Customer's written request, Elastic shall, subject to the parties executing an Order Form and Customer paying any applicable fees, continue to deliver a Cloud Service or make available the Software for a mutually agreed upon period following the termination of the applicable Subscription.

15. CONFIDENTIALITY.

Any information, responses and documentation provided by Elastic in connection with this Addendum, including the Certifications and Reports and Audit Results ("**Confidential Compliance Information**") shall be treated as Confidential Information of Elastic and shall be subject to the confidentiality obligations set forth in the Agreement. Without prejudice to the foregoing, Confidential Compliance Information may be disclosed to the Regulator, provided that Customer uses its reasonable efforts to obtain the agreement of the applicable Regulator to a non-disclosure agreement. If the Regulator refuses to sign a non-disclosure agreement, Customer shall inform the Regulator in writing of the confidential nature of the information to be made available to the Regulator.

16. COSTS & INSURANCE.

Customer shall bear all the reasonable costs and expenses arising from the exercise of the rights described in this Addendum regardless of whether it was exercised by the Customer or another party. Elastic shall maintain insurance with financially sound and reputable insurance companies in such amounts and against such risks as is customarily carried by responsible companies/firms in Elastic's industry engaged in similar businesses and in similar geographic areas. Elastic undertakes to provide, upon written request of the Customer and no more than once per year during the applicable Subscription Term, a copy of such insurance policy.

Exhibit A
Elastic Information Security Addendum

This Elastic Information Security Addendum ("**Addendum**") is subject to, and hereby incorporated into, the applicable agreement (including the applicable Data Processing Addendum entered into therewith) between Customer and Elastic for the Elastic Offerings (defined below) (the "**Agreement**"). This Addendum sets forth the terms and conditions related to Elastic's protection of Customer Information (as defined in the Agreement), including any Customer Personal Data therein, processed by Elastic within the Cloud Services, Support Services, and/or Consulting Services, as applicable ("**Elastic Offerings**"). Accordingly, Customer Information shall not be "Confidential Information" as such term is defined under the Agreement. Capitalized terms not defined in this Addendum shall have the meanings set forth in the applicable Agreement.

1. **INFORMATION SECURITY PROGRAM**. Elastic shall maintain an information security program that is designed to protect the security, confidentiality, and integrity of Customer Information (the "**Elastic Information Security Program**"). The Elastic Information Security Program will be implemented on an organization-wide basis. The Elastic Information Security Program will be designed to ensure Elastic's compliance with data protection laws and regulations applicable to Elastic's performance under the applicable Data Processing Addendum, and shall include the safeguards set forth on Appendix A, which substantially conform to the ISO/IEC 27002 control framework (the "Elastic Information Security Controls").

2. **THIRD-PARTY SERVICE PROVIDERS**. Customer acknowledges that Elastic does not maintain any physical data centers. Rather, Elastic uses Infrastructure as a Service (IaaS) providers, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to provide Elastic Cloud Services and uses Software as a Service Providers (SaaS), such as Salesforce, to provide Support Services and Consulting Services. Elastic shall conduct regular due diligence on its third party service providers (which includes reviewing industry standard reports and certifications such as a SOC 2 report), and reasonably assure itself, based on their responses, that such third parties have in place security controls that are substantially similar to the Elastic Information Security Controls.

3. **SECURITY BREACH RESPONSE**. Upon becoming aware of a confirmed Security Breach, Elastic shall: (a) without undue delay, notify Customer (at the Customer designated email address of the Organization Owner associated with the Elastic Offerings) of the discovery of the confirmed Security Breach, which shall include a summary of the known circumstances of the Security Breach and the corrective actions taken or to be taken by Elastic; (b) conduct an investigation of the circumstances of the Security Breach; (c) use commercially reasonable efforts to mitigate the effects of the Security Breach; and (d) use commercially reasonable efforts to communicate and cooperate with Customer concerning its responses to the Security Breach. "Security Breach" means any confirmed security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Information (including any Customer Personal Data contained therein) that Elastic has an obligation to safeguard under the Agreement.

4. **PROVISION OF SOC II, TYPE 2 REPORT**. Upon written request, Elastic shall provide to Customer copies of audit reports (including the Service Organization Control (SOC) II Type 2 examination or similar reports as Elastic may have obtained as of the date of the written request) applicable to the Elastic Offerings, and related certificates and attestations, evincing its compliance with industry standards and, as applicable, accreditations. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain compliance and accreditation. Upon Customer's request thereafter, Elastic shall provide current or updated certificates, attestations, or reports on up to an annual basis.

5. **SECURITY ASSESSMENT**. Upon the provision of reasonable notice to Elastic, once every twelve months during the term of the Agreement and during normal business hours, Elastic shall make appropriate Elastic personnel reasonably available to Customer to discuss Elastic's manner of compliance with applicable security obligations under this Agreement. In advance of such discussion, Elastic may, in its sole discretion, provide Customer with access to information or documentation concerning Elastic's information security practices as they relate to this Agreement, including without limitation, access to any security assessment reports designed to be shared with third parties. Any information or documentation provided pursuant to this assessment process or otherwise pursuant to this Addendum shall be considered Elastic Confidential Information and subject to the Confidentiality section of the Agreement.

6. **CLOUD SERVICES**. Notwithstanding anything contained herein, Customer shall be responsible for: (i) determining whether the Cloud Services are suitable for Customer's use; (ii) implementing and managing security and privacy measures to secure Customer's access and use of the Cloud Services, including, without limitation, managing credentials for and using secure connections to the Cloud Services; (iii) validating plugins before installing them into the Cloud Services; (iv) implementing, maintaining, and monitoring backups of Content stored within the Cloud Services; and (v) removing Content from the Cloud Services environment prior to termination of the relevant Cloud Service.

APPENDIX A ELASTIC INFORMATION SECURITY CONTROLS

SECURITY CONTROL CATEGORY	DESCRIPTION
1. Governance	a. Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing Elastic's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Customer Information. b. Use data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions.
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls. b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur.
3. Information Security Policies	a. Create information security policies, approved by management, published and acknowledged by all employees. b. Review and update policies at planned intervals to maintain their continuing suitability, adequacy, and effectiveness.
4. HR Security	a. Maintain policies requiring reasonable background checks of any new employee who will have access to Customer Information, subject to local law. b. Require all employees to undergo security awareness training on an annual basis.
5. Asset Management	a. Maintain a data classification standard based on data criticality and sensitivity. b. Maintain policies establishing data retention and secure destruction requirements. c. Implement procedures to clearly identify assets and assign ownership of those assets.
6. Access Controls	a. Maintain technical, logical, and administrative controls designed to limit access to Customer Information. b. For Cloud Services, restrict privileged access to the Content to authorized users with a business need. c. Review personnel access rights on a regular and periodic basis. d. Maintain policies requiring termination of access to Customer Information after termination of an employee. e. Implement access controls designed to authenticate users and limit access to Customer Information. f. Maintain multi-factor authentication processes for Elastic employees with access rights to systems containing Customer Information.
7. Cryptography	a. Implement encryption key management procedures. b. Encrypt Customer Information in transit and at rest using a minimum of AES-128 bit ciphers.
8. Physical Security	a. For Cloud Services, i. Implement controls designed to restrict unauthorized physical access to areas containing equipment used to provide the Cloud Services. ii. Maintain equipment used to host the Cloud Services in physical locations that are designed to be protected from natural disasters, theft, unlawful and unauthorized physical access, problems with ventilation, heating or cooling, and power failures or outages.
9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources. b. Contract with qualified independent third parties to perform periodic network and application penetration testing. c. Implement procedures to document and address vulnerabilities discovered during vulnerability and penetration tests.
10. Communications Security	a. For Cloud Services, require internal segmentation to isolate production systems hosting the Cloud Service from non-production networks. b. Require periodic reviews and testing of network controls. c. Centrally manage workstations via endpoint security solutions for deployment and management of end-point protections.

11. System Acquisition, Development, Maintenance	a. Assign responsibility for security, changes and maintenance for all information systems processing Customer Information. b. For Cloud Services, test, evaluate and authorize major information system components prior to implementation for the Cloud Service.
12. Information Security Incident Management	a. Monitor the access, availability, capacity and performance of the Cloud Service, Support Services and Consulting Services systems, and related system logs and network traffic using various monitoring software and services. b. Maintain incident response procedures for identifying, reporting, and acting on Security Breaches. c. Exercise the incident response process on a periodic basis. d. Implement plans to address gaps discovered during incident response exercises. e. Establish a cross-disciplinary security incident response team.
13. Business Continuity Management	a. Establish a cross-disciplinary security incident response team. Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. b. Conduct scenario-based testing annually.
14. Compliance	a Establish procedures designed to ensure all applicable statutory, regulatory, and contractual requirements are adhered to across the organization.

Exhibit B
Service Level Agreement

This Service Level Agreement ("**SLA**") is the primary document used to communicate Elastic's service level policy to Customer who is using a Cloud Service in a High Availability configuration under a fixed-term Subscription. Capitalized terms shall have the meanings specified below. Capitalized terms not defined in this below shall have the meanings set forth in the Agreement. Elastic reserves the right to reasonably modify the terms of this SLA during the Subscription Term. However, Elastic agrees not to materially diminish the service levels during the Subscription Term.

1. Availability Target. Elastic will use commercially reasonable efforts to make highly available Customer deployments on a Cloud Service available to the Customer with a Monthly Uptime Percentage of at least 99.95%, in each case during any full calendar month (the "**Cloud Service Availability Target**") during the Subscription Term. In the event Elastic does not meet the Cloud Service Availability Target, Customer will be eligible to receive a Service Credit as described below.

2. Definitions.

"**High Availability**" means that a deployment is running across at least two (2) availability zones.

"**Interval**" means a continuous period of five minutes.

"**Monthly Subscription Fee**" means the fees prepaid for the Usage Period in which the Unavailability occurred, divided by the number of months in that Usage Period.

"**Monthly Uptime Percentage**" is calculated per Cloud Service deployment, by subtracting from 100% the percentage of Intervals during a full calendar month in which the Cloud deployment was Unavailable.

"**Service Credit**" is a monetary credit, calculated as set forth below, that Elastic may credit back to an eligible account.

"**Unavailable**" means all continuous connection attempts to a High Availability deployment have failed during an Interval, provided the reason is not an Exclusion.

"**Unavailability**" means the state of being Unavailable.

"**Usage Period**" means that period of the Subscription Term during which prepaid Resources or credits are available for consumption.

3. Service Credits. Service Credits are calculated, in accordance with the schedule below, as a percentage of the applicable Monthly Subscription Fee, prorated for the fee contribution of the deployment(s) affected by the Unavailability to the overall fees for a Cloud Service usage in a given month:

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0% but equal to or greater than 95%	30%
Less than 95%	100%

Elastic will apply any Service Credits against future Cloud Service Gold, Platinum, Enterprise, or Private Subscription fees otherwise due from Customer. Service Credits will not entitle Customer to any refund or other payment from Elastic. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other Customer account, or transferred to any third party. Unless otherwise provided in the Agreement, Customer's sole and exclusive remedy for any Unavailability, non-performance, or other failure of a Cloud Service to meet the Cloud Service Availability Target, is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA. If availability is impacted by factors other than those used in Elastic's Monthly Uptime Percentage calculation, then Elastic may issue a Service Credit considering such factors at its discretion.

4. Credit Request and Payment Procedures. To receive a Service Credit, Customer must (1) open a ticket with the Elastic Support Center at support.elastic.co within 24 hours of first becoming aware of the applicable Unavailability and (2) within five (5) days of the applicable Unavailability, follow up on the initial ticket with a credit request that includes all of the following information:

- the words "**SLA Credit Request**" in the subject line;
- the dates and times of each Unavailability incident claimed by Customer;
- the affected account; and
- Customer's Request logs that document the errors and corroborate Customer's claim(s) of Unavailability outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by Elastic and is lower than a Cloud Service Availability Target, then Elastic will issue the Service Credit to Customer during the next applicable billing cycle following the month in which Customer's request is confirmed by Elastic. Customer's failure to provide the request and other information as required above will disqualify Customer from receiving a Service Credit.

5. Exclusions. The Monthly Uptime Percentage calculation does not take into account any Cloud Service Unavailability that is caused by, or results from, the following (collectively, "**Exclusions**"):

(i) a suspension or termination of Customer’s access to a Cloud Service in accordance with the Agreement;

(ii) factors outside of the reasonable control of Elastic, including any force majeure event or Internet access or related problems;

(iii) any actions or inactions of Customer or any third party, including failure to acknowledge a recovery volume, cluster misconfiguration, or lack of sufficient compute capacity sizing;

(iv) Customer’s equipment, software or other technology;

(v) third party equipment, software or other technology not under Elastic’s direct control (including, without limitation, third party cloud providers such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure used to host a Cloud Service);

(vi) Customer misconfiguring security groups, VPC configurations or credential settings, attempting to connect from an IP address not in the approved allowed list of IP addresses as configured by the customer, exceeding the number of connection limit, or client-side DNS issues;

(vii) Customer’s usage of a Cloud Service features that are no longer supported or that have been deprecated;

(viii) Customer’s usage of Elasticsearch versions that are no longer supported by a Cloud Service; or

(ix) Customer’s usage of preview, pre-release, beta, or trial versions of the Elasticsearch or a Cloud Service features.

Exhibit C
Microsoft Online Services current at the Effective Date of this Addendum

Microsoft Azure Core Services	Anomaly Detector, API Management, App Service (API Apps, Logic Apps, Mobile Apps, Web Apps), Application Gateway, Application Insights, Automation, Azure Active Directory (including Multi-Factor Authentication), Azure API for FHIR, Azure App Configuration, Azure Bot Services, Azure Cache for Redis, Azure Container Registry (ACR), Azure Container Service, Azure Cosmos DB (formerly DocumentDB), Azure Data Explorer, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Databricks, Azure DevOps Services, Azure DevTest Labs, Azure DNS, Azure Information Protection (including Azure Rights Management), Azure Kubernetes Service, Azure NetApp Files, Azure Resource Manager, Azure Search, Azure Spring Cloud, Azure Time Series Insights, Azure Video Analyzer for Media, Backup, Batch, BizTalk Services, Cloud Services, Computer Vision, Content Moderator, Custom Vision, Data Catalog, Data Factory, Data Lake Analytics, Data Lake Store, Event Hubs, Express Route, Face, Functions, HDInsight, Import/Export, IoT Hub, Key Vault, Language Understanding, Load Balancer, Log Analytics (formerly Operational Insights), Azure Machine Learning Studio, Media Services, Microsoft Azure Portal, Notification Hubs, Personalizer, Power BI Embedded, QnA Maker, Scheduler, Security Center, Service Bus, Service Fabric, SignalR Service, Site Recovery, Speech Services, SQL Data Warehouse, SQL Database, SQL Managed Instance, SQL Server Stretch Database, Storage, StorSimple, Stream Analytics, Synapse Analytics, Text Analytics, Traffic Manager, Translator, Virtual Machines, Virtual Machine Scale Sets, Virtual Network, and VPN Gateway

See here: https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all

Exhibit D
Subcontractor List

Cloud Service on AWS

Subcontractor	Service Provided	List of sub-subcontractors (if any)
AWS	Cloud hosting services	https://aws.amazon.com/compliance/sub-processors/

Cloud Service on MSFT

Subcontractor	Service Provided	List of sub-subcontractors (if any)
Microsoft	Cloud hosting services	https://go.microsoft.com/fwlink/p/?linkid=2096306

Cloud Service on GCP

Subcontractor	Service Provided	List of sub-subcontractors (if any)
Google	Cloud hosting services	https://cloud.google.com/terms/subprocessors