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.

	a. Require periodic reviews and testing of network controls. b. 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, 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.