Cloud Subscriptions Schedule

Information Security Measures Addendum

Supplier has implemented and will maintain the following security measures. These measures, in conjunction with the security measures outlined in the applicable Subscription Specification, are Supplier's only responsibility with respect to the security of the Supplier Offering. Unless otherwise defined in this document, all capitalized terms used in this document will have the meanings given to them in the Cloud Subscriptions Schedule.

Function	Measures
Information Security Program	Supplier has implemented and will maintain an information security program (including the adoption of internal policies and standards) that are designed to: (a) identify reasonably foreseeable security risks to the portions of the data centers, servers, networking equipment, firewalls, and host software systems that are within Supplier's control and used to provide the Supplier Offering ("**Supplier's Network**") and (b) mitigate identified security risks, where it deems appropriate, including through regular risk assessments and testing. Supplier has appointed one or more security officers responsible for coordinating, monitoring and enforcing the information security program. Supplier will maintain a threat and vulnerability management program that monitors for vulnerabilities in Supplier's Network on an on-going basis. Vulnerabilities are identified using a variety of sources/methods which may include vendors, security researchers, vulnerability scans, red team activities, penetration tests, and employee reporting. Publicly released third-party vulnerabilities are reviewed for applicability in the Supplier environment. Vulnerability scans and assessments are routinely and regularly performed on Supplier's application infrastructure. These processes are designed to enable proactive identification and remediation of vulnerabilities as well as support Supplier's compliance and regulatory requirements.
Secure Development Lifecycle & Vulnerability Response	Supplier has implemented and maintains a secure development lifecycle program to define the steps that must be taken to help ensure that its offerings have been appropriately designed, developed, and packaged under the structure of a formal governance program. This program, in concert with Supplier's information security program, helps to address security throughout the development and maintenance lifecycle of the Supplier Offering. Supplier employs a rigorous process to continually evaluate and improve its secure development and vulnerability response practices, and Supplier regularly compares these against industry standard practices. After investigating and validating a reported vulnerability in the Supplier Offering, Supplier will attempt to identify, develop, and qualify an appropriate remedy in accordance with Supplier's published vulnerability response policy, currently located at: Supplier Vulnerability Response Policy | Supplier US. Supplier communicates remedies to its customers through security advisories where applicable. Supplier strives to provide remedies in a commercially

	reasonable time. Response timelines will depend on many factors, such as: the severity of the vulnerability, the remedy complexity, or the component that is affected.
Asset Management	Supplier tracks physical and logical assets of Supplier's Network. Examples of the assets that Supplier may track, and controls that it may implement, include: (a) software assets, such as applications and system software, (b) physical assets, such as servers, desktops/laptops, backup/archival tapes, printers and communications equipment, and (c) information assets, such as databases, disaster recovery plans, business continuity plans, data classification and archived information. Supplier classifies assets based on business criticality and/or data classification sensitivity. Such classification allows for access to such asset to be appropriately restricted and managed.
Human Resources Security	As part of the employment process, Supplier employees are required to sign a non-disclosure agreement upon hire and undergo a screening process subject to and consistent with applicable law. Although Supplier reserves the right to review its policies and implement personnel security within its sole discretion, under current policy and subject to local law and local availability, Supplier conducts one or more of the following screenings for employment: drug screening, Social Security trace, criminal records search, education and employment verification, and employment eligibility verification. Supplier attempts to meet current industry standards for like companies in Supplier's industry, but Supplier cannot map its personnel security or screening process to meet the specific expectation of a particular Customer. Third parties or outside contractors are either screened by Supplier, screened as a condition of the contract, or verified as screened by the contractor following a Supplier-approved screening process. Supplier maintains a disciplinary process to take action against personnel that do not comply with its information security program requirements, including but not limited to, those put in place to meet its security, availability and confidentiality commitments and requirements. Supplier provides annual security awareness training to all applicable personnel and requires applicable subcontractors to provide such training for their personnel.
Physical Security	Risk-based controls are in place at facilities housing physical components of the Supplier's Network (e.g., data centers). Access controls may include security guards, security logs, monitoring, alarms, limited access to secure areas, protection of access paths, video surveillance, key cards, and/or two factor authentication. This provision applies to Supplier-managed Colocation Sites and vendor-managed data centers hosting public cloud services.
Network Security	Supplier's Network will be electronically accessible to Supplier's personnel as necessary to provide the Supplier Offering. Supplier will maintain policies and access controls to manage the access allowed to Supplier's Network from each

	connection, including the use of firewalls and authentication controls. Supplier protects against the malicious use of assets and malicious software in Supplier's Network, through the implementation of controls, based on risk. Such controls may include, but are not limited to: security polices; restrictive access controls; separate development and test environments; malware detection on servers, desktops and notebooks; malware email attachment scanning; system compliance scans; intrusion prevention monitoring and response; logging and alerting on key suspicious events; information handling procedures based on data type, e-commerce application and network security; use of external assets; and system and application vulnerability scanning. Supplier requires the encryption of data in transit and at rest where required and in accordance with its information security program. Supplier uses encryption and appropriate protocols (e.g. TLS) when remotely accessing a customer's environment or when transmitting customer data across open networks. Supplier stores its encryption keys, when not in use, in approved solutions designed to provide industry accepted key management practices.
Access Controls	Supplier implements appropriate access controls designed to protect against unauthorized access to Supplier's Network. To reduce the risk of misuse, intentional or otherwise, access to Supplier's Network is controlled following the principles of "least privilege" and "need to know". Access controls Supplier may utilize include access reviews, maintenance of service accounts and privileged access to the applications, system level settings for access, and the generation of access-related reports. Supplier utilizes industry standard practices, including, where applicable, two-factor authentication, to identify and authenticate Supplier's Network users. Supplier requires the use of strong passwords across Supplier's Network. Supplier (a) prohibits Supplier's Network users from sharing, writing down, emailing, IM'ing, or storing passwords unencrypted on any system, and (b) locks accounts after a series of consecutive incorrect password attempts. As appropriate, Supplier utilizes industry standard practices to enhance access controls including: (a) automatic time-out of user sessions if left idle, (b) identification and password requirement to reopen, (c) protection against external access by means of an accepted industry standard firewall(s) whose connection to the internet, if applicable, is safeguarded by a VPN connection; (d) masking of passwords when displayed or entered, as appropriate; and (e) appropriate and industry standard password encryption when transmitted.
Incident Management	Supplier utilizes an incident response framework to prepare for, respond to, manage and minimize the effects of security events. The framework includes procedures to be followed in the event of a security incident, including:

	(a) an internal incident response team with a response leader; (b) an investigation team performing root cause analysis and identifying affected parties; (c) internal reporting and notification processes; (d) documenting responsive actions and remediation plans; and (e) a post-incident review of events.
Business Continuity Management	Supplier maintains business continuity plans (“**BCP(s)**”) for recovering from a business interruption and resuming normal business operations as soon as reasonably practicable. Supplier will make reasonable and timely attempts, under the circumstances, to contact You in the event of a business interruption that materially impacts Supplier customers.