APEX Information Security Measures Addendum

The APEX Services use a shared security responsibility model in which You and Dell each have certain responsibilities, as they are hosted on Your premises or a Colocation Site and generally do not involve hosting of Customer Content on servers in Dell-managed data centers. Your responsibilities are specified in the applicable Service Offering Description.

Dell has implemented and will maintain the following corporate security measures for the APEX Services. These measures, in conjunction with the security measures outlined in the applicable Service Offering Description, are Dell's only responsibility with respect to the security of the APEX Services. Unless otherwise defined in this document, all capitalized terms used in this document will have the meanings given to them in the APEX Agreement.

Function	Measures
Information Security Program	Dell 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, if any, of Dell corporate data centers, servers, networking equipment, firewalls, and host software systems that are used to provide the APEX Services ("**Dell Network**"), and (b) use commercially reasonable efforts to mitigate identified security risks to the Dell Network, as and how Dell deems appropriate, including through regular risk assessments and testing. Dell has appointed one or more security officers responsible for coordinating, monitoring and enforcing the information security program. Dell will maintain a threat and vulnerability management program that monitors for vulnerabilities in the Dell 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 Dell environment. Vulnerability scans and assessments are routinely and regularly performed on Dell's application infrastructure. These processes are designed to enable proactive identification and remediation of vulnerabilities as well as support Dell's compliance and regulatory requirements.
Secure Development Lifecycle & Vulnerability Response	Dell has implemented and maintains a secure development life cycle program to define the steps that must be taken to help ensure that its offerings have been appropriately assessed, developed, and packaged under the structure of a formal governance program with a defined secure development lifecycle. This program, in concert with Dell's information security program, helps to address security throughout the development and maintenance lifecycle of the APEX System. Dell employs a rigorous process to continually evaluate and improve its secure development and vulnerability response practices, and Dell regularly compares these against industry standard practices. After investigating and validating a reported vulnerability in the APEX System, Dell will attempt to identify, develop, and qualify an appropriate remedy in

	accordance with Dell's published vulnerability response policy, currently located at https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy. Dell communicates remedies to its customers through security advisories where applicable. Dell strives to provide remedies in a commercially reasonable time, where applicable. Response timelines will depend on many factors, such as: the severity, the remedy complexity, or the component that is affected.
Asset Management	Dell tracks and manages physical and logical assets of the Dell Network. Examples of the assets that Dell 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. Dell classifies assets based on business criticality and/or data classification sensitivity. Such classification allows for access to such asset to be appropriately restricted.
Human Resources Security	As part of the employment process, Dell employees are required to sign a non-disclosure agreement upon hire and undergo a screening process subject to and consistent with applicable law. Although Dell 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, Dell 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. Dell attempts to meet current industry standards for like companies in Dell's industry, but Dell 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 Dell, screened as a condition of the contract, or verified as screened by the contractor following a Dell-approved screening process. Dell 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. Dell provides annual security awareness training to all applicable personnel and requires applicable subcontractors to provide such training for their personnel.
Physical Security	Dell maintains policies and controls which restrict physical access of facilities, where the physical components of the Dell Network are located, to authorized personnel and which aim to prevent the unauthorized entrance to the facilities.

	Risk based controls are in place at facilities housing physical components of the Dell 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 Dell managed Colocation Sites.
Network Security	The Dell Network is electronically accessible to Dell as necessary to provide the APEX Services. Dell will maintain policies and access controls to manage the access allowed to the Dell Network from each connection, including the use of firewalls and authentication controls. Dell protects against the malicious use of assets and malicious software in the Dell 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. Dell requires the encryption of data in transit and at rest where required and in accordance with its information security program. Dell uses encryption and appropriate protocols (e.g. TLS) when remotely accessing a customer system across open networks. Dell stores its encryption keys, when not in use, in approved solutions designed to provide industry accepted key management practices.
Access Controls	Dell implements appropriate access controls designed to protect against unauthorized access to the Dell Network. To reduce the risk of misuse, intentional or otherwise, access is controlled following the principles of “least privilege” and “need to know”. Access controls Dell 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. Dell utilizes industry standard practices, including, where applicable, two-factor authentication, to identify and authenticate Dell Network users. Dell requires the use of strong passwords across the Dell Network. Dell (a) prohibits Dell 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. Dell 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	Dell utilizes an incident response framework to prepare, respond to, manage and minimize the effects of security events. The framework includes procedures to be followed in the event of an 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	Dell maintains business continuity plans ("**BCP(s)**") for recovering from a business interruption and resuming normal business operations as soon as reasonably practicable. Dell will make reasonable and timely attempts, under the circumstances, to contact You in the event of a business interruption that materially impacts Your APEX Service(s).