Appendice alle misure per la sicurezza delle informazioni Dell APEX

I Servizi APEX prevedono un modello di responsabilità condivisa in materia di sicurezza in cui il Cliente e Dell assumono ciascuno determinate responsabilità; i Servizi APEX sono infatti in hosting presso la sede del Cliente o in Siti di colocation e generalmente non comportano l'hosting di Contenuti del Cliente su server in data center gestiti da Dell. Le responsabilità del Cliente sono specificate nella Descrizione del Servizio Offerto applicabile.

Dell ha implementato e si impegna a rispettare le seguenti misure di sicurezza aziendali per i Servizi APEX. Tali misure, unitamente alle misure di sicurezza illustrate nella Service Offering Description applicabile, rientrano nella responsabilità esclusiva di Dell relativamente alla sicurezza dei Servizi APEX. Salvo quanto diversamente specificato nel presente documento, tutti i termini con iniziale maiuscola devono essere interpretati secondo la relativa definizione fornita nel Contratto Dell APEX.

Funzione	Misure
Programma per la sicurezza delle informazioni	Dell ha implementato e si impegna a rispettare un programma per la sicurezza delle informazioni (compresa l'adozione di policy e standard interni) finalizzato a: (a) individuare i rischi per la sicurezza ragionevolmente prevedibili per eventuali componenti di data center, server, apparecchiature di rete, firewall e sistemi software host di Dell utilizzati per la fornitura dei Servizi APEX ("**Rete Dell**"); (b) fare quanto ragionevolmente possibile per mitigare i rischi individuati per la sicurezza della Rete Dell, nella misura e con le modalità ritenute opportune da Dell, anche attraverso regolari valutazioni e verifiche del rischio. Dell ha nominato uno o più funzionari responsabili della sicurezza al fine di coordinare, monitorare e attuare il programma per la sicurezza delle informazioni. Dell si impegna ad applicare un programma di gestione delle minacce e delle vulnerabilità in grado di monitorare costantemente le vulnerabilità della Rete Dell. Le vulnerabilità vengono identificate grazie a una serie di fonti/metodi che possono includere fornitori, esperti di sicurezza, analisi delle vulnerabilità, attività di red team, penetration test e segnalazioni dei dipendenti. Le vulnerabilità di terze parti rese pubbliche sono sottoposte a revisione per verificarne l'applicabilità in ambiente Dell. Sull'infrastruttura applicativa di Dell vengono eseguite regolarmente analisi e valutazioni delle vulnerabilità. Tali procedure sono concepite per consentire l'identificazione e la correzione proattiva delle vulnerabilità e soddisfare i requisiti Dell di conformità e richiesti dalle normative vigenti.
Ciclo di vita dello sviluppo sicuro e risposta alle vulnerabilità	Dell ha implementato e si impegna a rispettare un programma di ciclo di vita dello sviluppo sicuro per definire misure volte a garantire che le sue offerte siano valutate, sviluppate e commercializzate in modo appropriato nell'ambito di un programma di governance formale, con un ciclo di vita dello sviluppo sicuro ben definito. Questo programma, di concerto con il programma per la sicurezza delle informazioni di Dell, contribuisce a garantire la sicurezza durante l'intero ciclo di vita di sviluppo e manutenzione del sistema APEX. Dell attua un processo rigoroso per valutare e migliorare costantemente le proprie pratiche di sviluppo sicuro e di risposta alle vulnerabilità, confrontandole regolarmente con le pratiche standard del settore.

	Dopo aver esaminato e verificato una vulnerabilità segnalata nel Sistema APEX, Dell si adopera per individuare, sviluppare e definire un rimedio appropriato in conformità alla sua politica di risposta alle vulnerabilità pubblicata, attualmente reperibile all'indirizzo https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy. Ove opportuno, Dell comunica ai propri clienti eventuali misure correttive tramite avvisi di sicurezza. Dell si impegna a fornire misure correttive in tempi ragionevoli, ove possibile. Le tempistiche di risposta dipendono da molti fattori, quali la gravità, la complessità delle misure correttive o il componente interessato.
Gestione degli asset	Dell traccia e gestisce gli asset fisici e logici della Rete Dell. Di seguito sono riportati alcuni esempi di asset tracciati e di controlli che Dell può implementare: (a) asset relativi al software, come applicazioni e software di sistema; (b) asset fisici, come server, desktop/laptop, nastri di backup/ archiviazione, stampanti e apparecchiature di comunicazione; e (c) asset informativi, come database, piani di ripristino di emergenza, piani di continuità aziendale, classificazione dei dati e informazioni archiviate. Dell classifica gli asset in base alla criticità per l'azienda e/o alla sensibilità di classificazione dei dati. Tale classificazione consente di limitare adeguatamente l'accesso ai singoli asset.
Sicurezza delle risorse umane	Nell'ambito del processo di assunzione, i dipendenti Dell sono tenuti a sottoscrivere un accordo di non divulgazione al momento dell'assunzione e a sottoporsi a una procedura di screening soggetta e conforme alle leggi vigenti. Fatta salva la facoltà di Dell di rivedere le proprie policies e attuare le misure di sicurezza del personale a propria discrezione, in conformità alla policy attuale, alle leggi locali e secondo la disponibilità locale, Dell effettua uno o più dei seguenti screening per l'assunzione: screening per l'uso di sostanze stupefacenti, tracciamento dei dati di previdenza sociale, ricerca di precedenti penali, verifica della formazione e dell'esperienza professionale e verifica dell'idoneità all'impiego. Dell si impegna a rispettare gli attuali standard del settore per le aziende analoghe del suo comparto, ma non è in grado di configurare le proprie procedure di sicurezza o di selezione del personale in modo da soddisfare le specifiche aspettative di un particolare Cliente. Appaltatori esterni o soggetti terzi sono sottoposti a screening da parte di Dell, come condizione contrattuale o confermati dall'appaltatore come verificati a seguito di un processo di screening approvato da Dell. Dell applica un processo disciplinare per l'adozione di provvedimenti nei confronti del personale che non rispetta i requisiti del programma per la sicurezza delle informazioni, compresi, a titolo esemplificativo, eventuali provvedimenti messi in atto per soddisfare gli impegni e i requisiti di sicurezza, disponibilità e riservatezza. Dell offre a tutto il personale interessato una formazione annuale di consapevolezza sulla sicurezza e richiede ai subappaltatori interessati di fornire tale formazione al proprio personale.

Sicurezza fisica	Dell adotta policies e controlli finalizzati a limitare l'accesso fisico alle strutture in cui sono collocati i componenti fisici della Rete Dell unicamente al personale autorizzato e impedirne l'ingresso a chi non sia autorizzato. Presso le strutture che ospitano componenti fisici della Rete Dell (ad esempio, i data center) vengono effettuati controlli basati sul rischio. Tali controlli possono includere guardie giurate, registri di sicurezza, monitoraggio, allarmi, accesso limitato alle aree protette, protezione dei percorsi di accesso, videosorveglianza, badge e/o autenticazione a due fattori. Questa disposizione si applica ai Siti di colocation gestiti da Dell.
Sicurezza della rete	La Rete Dell è accessibile elettronicamente a Dell nella misura necessaria a fornire i Servizi APEX. Dell manterrà policy e sistemi di controllo degli accessi per gestire l'accesso consentito alla Rete Dell da ciascuna connessione, incluso l'uso di firewall e controlli di autenticazione. Dell previene l'uso illecito di asset e software malevoli all'interno della Rete Dell tramite l'implementazione di controlli, in base al rischio. Tali controlli possono includere, in via esemplificativa: policies di sicurezza, un sistema rigoroso di controllo degli accessi, ambienti di sviluppo e test separati, rilevamento di malware su server, desktop e notebook, scansione anti-malware degli allegati alle e-mail, scansioni per la conformità dei sistemi, monitoraggio per la prevenzione delle intrusioni ed eventuale risposta, registrazione e allerta in merito a eventi sospetti chiave, procedure di trattamento delle informazioni in base al tipo di dati, sicurezza della rete e applicazioni di e-commerce, uso di asset esterni e scansione della vulnerabilità di sistema e applicazioni. Dell richiede la crittografia dei dati in transito e at-rest laddove necessario e conformemente al programma per la sicurezza delle informazioni. Dell utilizza la crittografia e protocolli adeguati (ad es. TLS) per l'accesso da remoto al sistema di un cliente su reti aperte. Quando non sono in uso, Dell conserva le chiavi di crittografia in soluzioni approvate, concepite per garantire l'implementazione di pratiche accettate dal settore per la gestione delle chiavi.
Controlli degli accessi	Dell implementa adeguati sistemi di controllo degli accessi, concepiti per prevenire l'accesso non autorizzato alla Rete Dell. Per ridurre il rischio di uso improprio, intenzionale o meno, l'accesso viene controllato secondo i principi di "privilegio minimo" e "need-to-know". I sistemi di controllo degli accessi che Dell può adottare includono: verifiche degli accessi, mantenimento di account di servizio e accesso con privilegi alle applicazioni, impostazioni di accesso a livello di sistema e generazione di report sugli accessi. Dell impiega pratiche standard del settore tra cui, ove opportuno, l'autenticazione a due fattori, per identificare e autenticare gli utenti della Rete Dell. Dell richiede l'uso di password complesse nell'intera Rete Dell. Dell (a) vieta agli utenti della Rete Dell la condivisione, la copia per iscritto, l'invio tramite e-mail o sistemi di messaggistica interni o l'archiviazione di password non crittografate su qualsiasi sistema e (b) blocca gli account dopo una serie di tentativi consecutivi falliti di immissione della password. Per migliorare il controllo degli accessi, Dell si avvale di pratiche standard del settore, tra cui: (a) time-out automatico delle sessioni utente lasciate inattive;

	(b) obbligo di identificazione e password per la riapertura; (c) protezione contro l'accesso da parte di soggetti esterni per mezzo di uno o più firewall standard del settore, la cui connessione a Internet, se del caso, è protetta tramite VPN; (d) mascheramento delle password quando vengono visualizzate o inserite, a seconda dei casi; e (e) crittografia delle password appropriata e conforme agli standard del settore al momento della trasmissione.
Incident Management	Dell adotta una strategia di risposta agli incidenti volta a prevenire, rispondere, gestire e ridurre al minimo gli effetti di eventi legati alla sicurezza. Il quadro di riferimento comprende le procedure da seguire in caso di incidente di sicurezza, tra cui: (a) un team interno di risposta agli incidenti con un responsabile incaricato di rispondere; (b) un team investigativo che esegue la root-cause analysis e individua le parti interessate; (c) procedure interne di segnalazione e notifica; (d) la documentazione delle azioni di risposta e dei piani correttivi; inoltre (e) una revisione degli eventi dopo l'incidente.
Gestione della continuità aziendale	Dell attua piani di continuità aziendale ("**BCP",** Business Continuity Plan) per il ripristino da un'interruzione dell'attività e la ripresa delle normali operazioni aziendali non appena ragionevolmente possibile. In funzione delle circostanze, Dell farà tutto il possibile al fine di contattare il cliente in modo tempestivo qualora si verifichi un'interruzione della continuità aziendale che abbia un impatto sostanziale sui Servizi APEX del Cliente.