

Contratto per Offerte di Servizi Cloud

Appendice alle misure di sicurezza delle informazioni

Dell ha implementato e si impegnerà a rispettare le seguenti misure di sicurezza aziendali. Tali misure, unitamente alle misure di sicurezza illustrate nella Descrizione del Servizio Offerto applicabile, rientrano nella responsabilità esclusiva di Dell relativamente alla sicurezza dell'Offerta di Servizi. Salvo diversamente specificato nel presente documento, tutti i termini con iniziale maiuscola devono essere interpretati secondo la relativa definizione fornita nel Contratto per Offerte di Servizi Cloud.

Funzione	Misure
<p>Programma per la sicurezza delle informazioni</p>	<p>Dell ha implementato e si impegnerà a rispettare un programma per la sicurezza delle informazioni (compresa l'adozione di politiche e standard interni) finalizzato a:</p> <ul style="list-style-type: none"> (a) individuare i rischi per la sicurezza ragionevolmente prevedibili per eventuali componenti dei data center aziendali, server, apparecchiature di rete, firewall e sistemi software host di Dell utilizzati per l'Offerta di Servizi ("Rete Dell") e (b) ridurre i rischi identificati, laddove ritenuto appropriato, incluse attività regolari di assessment dei rischi. <p>Dell ha nominato uno o più funzionari responsabili della sicurezza al fine di coordinare, monitorare e attuare il programma per la sicurezza delle informazioni.</p> <p>Dell si impegnerà 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.</p>
<p>Ciclo di vita dello sviluppo sicuro e risposta alle vulnerabilità</p>	<p>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 dell'Offerta di Servizi. 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 nell'Offerta di Servizi, Dell si adopererà per individuare, sviluppare e definire un rimedio appropriato in conformità alla sua politica di risposta alle vulnerabilità pubblicata, attualmente disponibile alla pagina Policy di risposta Dell alle vulnerabilità</p>

	<p>Se del caso, Dell comunica ai propri clienti eventuali rimedi tramite avvisi di sicurezza. Dell si impegna a fornire rimedi in tempi commercialmente ragionevoli, ove possibile. Le tempistiche di risposta dipendono da molti fattori, quali la gravità, la complessità del rimedio o il componente interessato.</p>
Gestione degli asset	<p>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:</p> <p>(a) asset relativi al software, ad esempio applicazioni e software di sistema;</p> <p>(b) asset fisici, ad esempio server, desktop/laptop, nastri di backup/archiviazione, stampanti e apparecchiature di comunicazione; infine</p> <p>(c) asset informativi, ad esempio database, piani di ripristino di emergenza, piani di continuità aziendale, classificazione dei dati e informazioni archiviate.</p> <p>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.</p>
Sicurezza delle risorse umane	<p>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. Nonostante il diritto riservato di rivedere le proprie politiche e attuare le misure di sicurezza del personale a propria discrezione, in conformità alla politica attuale e 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 può configurare le proprie procedure di sicurezza o di selezione del personale al fine di soddisfare le specifiche aspettative di un particolare Cliente.</p> <p>Appaltatori esterni o soggetti terzi sono sottoposti a screening da parte di Dell o come condizione contrattuale o attestati come tali dall'appaltatore a seguito di un processo di screening approvato da Dell.</p> <p>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.</p> <p>Dell offre una formazione annuale di sensibilizzazione alla sicurezza a tutto il personale interessato e richiede ai subappaltatori di fornire tale formazione al proprio personale.</p>
Sicurezza fisica	<p>Dell adotta policy e controlli al fine di impedire l'ingresso non autorizzato alle strutture in cui sono collocati i componenti fisici della Rete Dell e di consentire l'accesso fisico unicamente al personale autorizzato.</p> <p>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,</p>

	<p>accesso limitato alle aree protette, protezione dei percorsi di accesso, videosorveglianza, badge e/o autenticazione a due fattori.</p> <p>Questa disposizione si applica ai Siti di Colocation gestiti da Dell.</p>
<p>Sicurezza della rete</p>	<p>La Rete Dell sarà accessibile elettronicamente al personale Dell nella misura necessaria a erogare l'Offerta di Servizi. Dell adotterà 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.</p> <p>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: politiche 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.</p> <p>Dell richiede la crittografia dei dati in transito e a riposo 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 o per la trasmissione di informazioni personali 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 le attività di gestione principali.</p>
<p>Controlli degli accessi</p>	<p>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" (accesso limitato alle sole informazioni necessarie). 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.</p> <p>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.</p> <p>Per migliorare il controllo degli accessi, Dell si avvale di pratiche standard del settore, tra cui:</p> <ul style="list-style-type: none"> (a) time-out automatico delle sessioni utente lasciate inattive; (b) obbligo di identificazione e password per la riapertura;

	<p>(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;</p> <p>(d) mascheramento delle password quando vengono visualizzate o inserite, a seconda dei casi; inoltre</p> <p>(e) crittografia appropriata e conforme agli standard industriali delle password quando vengono trasmesse.</p>
<p>Incident Management</p>	<p>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:</p> <p>(a) un team interno di risposta agli incidenti con un responsabile incaricato di rispondere;</p> <p>(b) un team investigativo che esegue l'analisi delle cause principali e individua le parti interessate;</p> <p>(c) procedure interne di segnalazione e notifica;</p> <p>(d) la documentazione delle azioni di risposta e dei piani di correzione; inoltre</p> <p>(e) una revisione degli eventi dopo l'incidente.</p>
<p>Gestione della continuità aziendale</p>	<p>Dell mette in atto 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. Date le 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 clienti Dell.</p>