POLITICA PER LA SICUREZZA DELLE INFORMAZIONI, PROTEZIONE DEI DATI E BUSINESS CONTINUITY

La gestione della sicurezza delle informazioni può essere definita come l'insieme delle misure tecnologiche, organizzative, procedurali e legali che consentono a un'organizzazione di identificare, valutare e gestire i rischi ai quali sono sottoposti i sistemi informativi, le infrastrutture tecnologiche, i dati e i servizi erogati.

Nell'era della digitalizzazione, la crescente diffusione di tecnologie innovative come l'AI e l'interconnessione dei sistemi richiedono l'elaborazione di strategie capaci di coniugare gli obiettivi di sviluppo sostenibile con il rafforzamento della sicurezza informatica, garantendo adeguati livelli di resilienza operativa e continuità dei servizi essenziali.

La centralità del progresso tecnologico e la necessità di garantirne la sicurezza, nel rispetto della sostenibilità ambientale, sociale ed economica, rivestono oggi un ruolo cruciale e richiedono un impegno costante per mantenere un equilibrio tra innovazione, protezione delle informazioni, resilienza operativa e conformità normativa.

Telebit riconosce l'importanza di valutare le esigenze e le aspettative delle parti interessate, inclusi clienti, fornitori, partner, dipendenti, autorità competenti e stakeholder istituzionali, anche con riferimento agli impatti derivanti dal cambiamento climatico, dagli scenari geopolitici e dalle minacce cyber emergenti.

Tali aspetti sono pertanto inclusi nella regolare analisi del contesto interno ed esterno e nella valutazione dei rischi aziendali.

La **Politica Integrata di Telebit** costituisce parte integrante del Sistema di Gestione Integrato aziendale, di cui la Sicurezza delle Informazioni, la Cybersecurity e la Business Continuity rappresentano elementi fondamentali.

Tali ambiti contribuiscono al raggiungimento degli Obiettivi di Sviluppo Sostenibile (SDGs), in particolare:

- **SDG 9 – Industria, innovazione e infrastrutture**, attraverso il rafforzamento della resilienza delle infrastrutture informative e operative;
- **SDG 16 – Pace, giustizia e istituzioni solide**, mediante la protezione dei dati, la gestione trasparente dei rischi e il rafforzamento della fiducia degli stakeholder;
- **SDG 8 – Lavoro dignitoso e crescita economica**, garantendo la continuità operativa (business continuity), la tutela dei livelli occupazionali e la stabilità economica dell'Organizzazione anche in presenza di minacce informatiche.

La presente Politica, sottoscritta dal **CIO** (Chief Information Officer) e approvata dalla **Direzione Telebit**, stabilisce gli indirizzi strategici per la protezione delle informazioni, la resilienza operativa, la gestione degli incidenti informatici e la conformità alle norme ISO/IEC 22301 e ISO/IEC 27001, nonché alle disposizioni applicabili derivanti dalla Direttiva NIS2 e dalla normativa nazionale vigente.

La presente Politica si fonda sui principi di:

- **Riservatezza**: garantire che le informazioni siano accessibili esclusivamente ai soggetti autorizzati; applicazione del principio di Need to Know
- **Integrità**: proteggere accuratezza, completezza e affidabilità delle informazioni e dei processi di trattamento;
- **Disponibilità**: assicurare che le informazioni, i sistemi e i servizi siano disponibili agli utenti autorizzati quando necessario;
- **Resilienza**: assicurare la capacità di **Telebit** di prevenire, resistere, rispondere e riprendersi da eventi avversi, incidenti cyber e situazioni di emergenza.

Telebit è consapevole che la mancanza di adeguati livelli di sicurezza e resilienza può comportare danni reputazionali, interruzioni operative, perdita di dati, compromissione dei servizi, violazioni normative, sanzioni amministrative, danni economici e finanziari nonché impatti negativi sulle parti interessate e sulla continuità aziendale.

Tutti gli asset aziendali, materiali (edifici, impianti, infrastrutture, dispositivi, reti, persone) e immateriali (informazioni, dati, software, know-how, organizzazione, servizi e processi di business), sono protetti attraverso strategie di sicurezza proporzionate al livello di rischio, definite mediante specifiche politiche, procedure e controlli organizzativi e tecnologici finalizzati a mantenere *il corretto equilibrio tra rischio, valore e costi di protezione*.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI, PROTEZIONE DEI DATI E BUSINESS CONTINUITY

Telebit promuove un *approccio integrato* alla Sicurezza delle Informazioni e alla Business Continuity, attraverso il coordinamento tra le funzioni aziendali coinvolte nella gestione delle infrastrutture tecnologiche, della sicurezza informatica, della protezione dei dati, della continuità operativa e della gestione dei rischi.

La sicurezza delle informazioni e la resilienza operativa sono perseguite mediante un processo strutturato di gestione del rischio che prevede:

- l'identificazione e classificazione degli asset critici;
- la valutazione periodica delle minacce, vulnerabilità e impatti;
- l'adozione di misure tecniche e organizzative adeguate;
- il monitoraggio continuo dei rischi cyber e operativi;
- il miglioramento continuo delle misure di sicurezza;
- la verifica periodica dell'efficacia dei controlli implementati.

All'interno di **Telebit** la sicurezza delle informazioni, la cybersecurity e la Business Continuity sono garantite attraverso le seguenti misure:

- Il personale conosce e applica le policy e le procedure aziendali relative alla sicurezza delle informazioni, alla cybersecurity, alla protezione dei dati e alla continuità operativa.
- Il personale è oggetto di attività periodiche di formazione, sensibilizzazione e aggiornamento sui rischi cyber, sulle minacce emergenti, sul phishing, sulla protezione delle informazioni e sulla gestione degli incidenti.
- Le informazioni e le registrazioni aziendali sono archiviate e gestite in modo da garantirne rintracciabilità, integrità, disponibilità e protezione.
- Tutti i software utilizzati dispongono di regolari licenze e sono soggetti a monitoraggio, manutenzione e aggiornamento periodico.
- I Data Center e le infrastrutture critiche sono protetti mediante adeguati controlli fisici e logici per prevenire accessi non autorizzati.
- I sistemi sono progettati e mantenuti per garantire resilienza, continuità operativa e capacità di ripristino in caso di guasto, incidente o attacco informatico.
- L'accesso ai sistemi e alle reti aziendali avviene attraverso processi di autenticazione sicuri e meccanismi di autorizzazione basati sul principio del minimo privilegio.
- Sono adottati strumenti di monitoraggio, rilevamento e prevenzione delle minacce informatiche, inclusi firewall, sistemi IDS/IPS, sistemi antivirus, sistemi di logging e monitoraggio degli eventi di sicurezza.
- I log e le registrazioni di sicurezza sono raccolti, protetti e conservati nel rispetto delle normative applicabili, al fine di garantire tracciabilità e supportare le attività di analisi e risposta agli incidenti.
- I dati aziendali sono sottoposti a backup periodici e protetti mediante adeguate misure di cifratura, conservazione sicura e procedure di ripristino testate regolarmente.
- Le connessioni remote e gli accessi dall'esterno sono protetti tramite protocolli sicuri, autenticazione forte e controlli di accesso adeguati.
- Le modifiche ai sistemi, alle infrastrutture e agli applicativi sono gestite mediante processi strutturati di Change Management finalizzati a ridurre il rischio di vulnerabilità o interruzioni operative.
- Gli incidenti informatici e gli eventi di sicurezza sono registrati, gestiti, analizzati e classificati secondo procedure formalizzate, prevedendo escalation interne, azioni correttive e, ove applicabile, notifiche alle autorità competenti nei tempi previsti dalla normativa vigente.
- Le procedure di Business Continuity e Disaster Recovery sono periodicamente testate e aggiornate per garantire la continuità dei servizi essenziali e il rapido ripristino delle attività.
- Gli impianti ausiliari e le infrastrutture di supporto dei Data Center sono soggetti a manutenzione preventiva e correttiva programmata.

Telebit valuta periodicamente i rischi derivanti dalla supply chain ICT e dai fornitori critici, adottando misure di controllo, requisiti di sicurezza contrattuali e processi di monitoraggio dei fornitori rilevanti ai fini della cybersecurity e della continuità operativa.

Telebit promuove un approccio orientato al miglioramento continuo, alla resilienza digitale e alla conformità normativa, anche attraverso audit interni, verifiche periodiche, esercitazioni e simulazioni di gestione delle crisi e degli incidenti cyber.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI, PROTEZIONE DEI DATI E BUSINESS CONTINUITY

Telebit ha investito non solo nelle infrastrutture tecnologiche e nelle procedure operative, ma anche nello sviluppo di competenze specialistiche e risorse dedicate alla sicurezza delle informazioni, alla cybersecurity, alla protezione dei dati e alla Business Continuity, individuando specifici ruoli e responsabilità organizzative.

Per quanto attiene alle informazioni aziendali e dei clienti di cui venga a conoscenza nel corso delle proprie attività, tutto il personale di **Telebit** è soggetto agli obblighi di riservatezza previsti dal CCNL, dalla lettera di assunzione, dalle policy aziendali, dai requisiti contrattuali dei clienti e dalle normative vigenti.

Analogamente, eventuali fornitori, partner o terze parti che dovessero venire a conoscenza di informazioni riservate o accedere a sistemi e dati aziendali sono vincolati da specifici obblighi contrattuali di riservatezza, sicurezza delle informazioni, protezione dei dati e continuità operativa, in conformità ai requisiti normativi applicabili e agli standard adottati da **Telebit**.

Dosson di Casier, 07/05/2026

CIO
Chief Information Officer
Andre Costa

Legale Rappresentante
Giacomo Quarta

telebit S.p.A.
Legale Rappresentante
QUARTA GIACOMO