Politica sulla
Security Awareness

Data di emissione	28 giugno 2024
Classe di riservatezza	Documento interno
Riferimenti	Leggi in materia di Sicurezza delle Informazioni e documenti interni
Approvatore	Benedetto Di Salvo, *Chief Executive Officer*

Indice dei Contenuti

Definizioni

- **Confidenzialità:** proprietà dell'informazione che assicura che l'informazione non sia resa disponibile o divulgata a individui, entità o processi non autorizzati. È uno dei tre pilastri fondamentali della sicurezza delle informazioni, insieme all'integrità e alla disponibilità. Garantire la confidenzialità significa proteggere le informazioni sensibili e riservate da accessi non autorizzati, sia intenzionali che accidentali.
- **Integrità:** proprietà di accuratezza e completezza delle informazioni. È uno dei tre pilastri fondamentali della sicurezza delle informazioni, insieme alla confidenzialità e alla disponibilità. Assicurare l'integrità significa proteggere le informazioni da modifiche non autorizzate, garantendo che i dati siano accurati e completi durante l'intero ciclo di vita, inclusi i processi di archiviazione, trasmissione e recupero.
- **Disponibilità:** proprietà dell'informazione di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato. È uno dei tre pilastri fondamentali della sicurezza delle informazioni, insieme alla confidenzialità e all'integrità. Garantire la disponibilità significa che i sistemi che ospitano le informazioni devono essere operativi e i dati devono essere accessibili nei tempi richiesti per soddisfare le esigenze aziendali, senza interruzioni indebite.
- **Information Security Management System (ISMS)**: approccio sistematico e strutturato alla gestione della sicurezza delle informazioni all'interno di un'organizzazione. L'obiettivo principale di un ISMS è proteggere la confidenzialità, l'integrità e la disponibilità delle informazioni, garantendo al contempo la gestione dei rischi associati.
- **Serie ISO/IEC 27000**: comprende gli standard di sicurezza delle informazioni che si supportano reciprocamente e che insieme forniscono un quadro riconosciuto a livello globale delle best practice per la gestione della sicurezza delle informazioni (Information Security Management System - ISMS). Standard internazionale per la gestione della sicurezza delle informazioni, in particolare, la ISO/IEC 27001 fornisce un quadro di riferimento dettagliato per la progettazione, l'implementazione, il monitoraggio e il miglioramento continuo di un sistema di gestione della sicurezza delle informazioni all'interno di un'organizzazione.
- **Direttiva NIS2**: "Network and Information Systems 2" (Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022) direttiva europea che stabilisce una linea di base di misure di sicurezza informatica per le organizzazioni del settore pubblico e privato che forniscono servizi essenziali legati alla cyber security.
- **Security Awareness**: grado di conoscenza e comprensione che le persone hanno riguardo alle questioni relative alla sicurezza, specialmente in contesti informatici e di protezione delle informazioni. In un contesto più ampio, la security awareness può estendersi alla consapevolezza generale della sicurezza fisica, della privacy e di altri aspetti legati alla sicurezza.
- **Security Awareness Program**: iniziativa organizzativa progettata per educare e sensibilizzare gli utenti e il personale su questioni cruciali legate alla sicurezza delle informazioni e per promuovere comportamenti sicuri. L'obiettivo principale di un programma di consapevolezza sulla sicurezza è ridurre i rischi associati a errori umani, comportamenti negligenti o attacchi mirati attraverso l'incremento della consapevolezza e della comprensione delle minacce e delle migliori pratiche di sicurezza.

  Incidente di sicurezza: qualsiasi violazione digitale o fisica che minacci la confidenzialità, integrità o disponibilità dei sistemi informativi o dei dati sensibili di Italtel.

1. Scopo

La presente politica (di seguito “policy”) ha lo scopo di:

- promuovere, nell’ambito dell’*Information Security Management System* (ISMS) e del *Security Awareness Program*, una cultura della sicurezza all'interno di Italtel S.p.A. (nel seguito, anche “Italtel”);
- sensibilizzare tutti i dipendenti, i collaboratori e le terze parti, circa i rischi relativi alla sicurezza delle informazioni, affinché tutti siano consapevoli delle pratiche di sicurezza dell'informazione e agiscano in conformità con i requisiti delle norme applicabili.

2. Campo di applicazione

La presente policy si applica a tutti i dipendenti Italtel, ai collaboratori e alle terze parti che agiscono in nome e per conto di Italtel, e che hanno accesso ai dati e ai sistemi di Italtel.

3. Documenti di riferimento

Italtel, in compliance con le norme applicabili in materia di sicurezza delle informazioni, dispone di specifiche informative, procedure e istruzioni operative, messe a disposizione di tutto il personale in aree accessibili (es. intranet aziendale) e delle terze parti che operano in nome e per conto di Italtel.

La presente policy rimanda ai seguenti documenti nei quali sono opportunamente trattati specifici temi relativi alla gestione della sicurezza delle informazioni:

- Politica sulla Sicurezza delle Informazioni
- Politica sul corretto utilizzo delle risorse informatiche aziendali
- Regole per lo svolgimento del lavoro da remoto (Smart Working)
- Gestione delle password – Istruzione Operativa
- Gestione degli incidenti - Linea Guida
- Gestione degli incidenti informatici – Istruzione Operativa

4. Ruoli e responsabilità

Tutti gli utenti dell'organizzazione sono componenti fondamentali della promozione della cultura della *Security awareness* e, pertanto, sono chiamati all’applicazione delle regole di sicurezza delle informazioni e al rispetto delle stesse nell’utilizzo delle risorse informatiche aziendali.

Si riportano nella seguente tabella le responsabilità di ciascuna funzione aziendale nell’ambito del *Security Awareness Program*.

Funzione/ruolo	Responsabilità
Direzione e Management	Promuovere una cultura di sicurezza delle informazioni in tutta l'organizzazione. Ciò include l'allocazione di risorse adeguate alla formazione e la consapevolezza della sicurezza. Tutti i Manager sono responsabili di garantire che i propri collaboratori partecipino attivamente nella diffusione della Security Awareness, applicando le regole contenute nelle policy, procedure e istruzioni operative relative alla Sicurezza delle informazioni.

Responsabile del Sistema di Gestione della Sicurezza dell'informazione (SGSI)	Progettare, implementare e valutare le iniziative di formazione e consapevolezza della sicurezza dell'informazione. In particolare, è responsabile di: ▪ definire obiettivi di consapevolezza misurabili e indicatori chiave di performance (KPI) per valutare l'efficacia delle iniziative di sicurezza informatica; ▪ collaborare con HR&O nella progettazione e nell'implementazione di programmi di formazione sulla sicurezza; ▪ partecipare alla valutazione dei rischi di sicurezza informatica e identificare aree in cui la consapevolezza della sicurezza può essere rafforzata per mitigare specifiche minacce.
Internal Audit & Compliance	Assicurare che la Security Awareness Policy sia implementata in modo efficace, valutandone la conformità, identificandone i rischi e contribuendo alla creazione di un ambiente sicuro e consapevole all'interno dell'organizzazione. Collaborare con la Direzione e il Responsabile del Sistema di Gestione della Sicurezza dell'Informazione (SGSI) per garantire che la Security Awareness Policy sia sostenibile nel tempo. Partecipare all'adattamento della politica in risposta a cambiamenti nei rischi di sicurezza e alle normative pertinenti. In particolare, è responsabile di: ▪ valutare la conformità dell'organizzazione alla Security Awareness Policy; ▪ verificare se i dipendenti e le terze parti rispettano le linee guida contenute nelle policy e procedure connesse alla presente policy; ▪ fornire rapporti dettagliati sulla conformità, evidenziando aree di forza e di debolezza nella sicurezza dell'informazione; ▪ monitorare costantemente l'efficacia delle iniziative di formazione e consapevolezza, fornendo feedback utili per il miglioramento continuo; ▪ contribuire all'identificazione e alla valutazione dei rischi relativi alla sicurezza dell'informazione attraverso analisi dettagliate e audit;

	▪ segnalare potenziali minacce alla sicurezza informatica e aiutare a sviluppare strategie per mitigare questi rischi attraverso azioni correttive; ▪ offrire formazione supplementare quando necessario, basata sui risultati delle valutazioni e degli audit; ▪ interagire con enti di regolamentazione esterni e agenzie di certificazione per garantire la conformità ai requisiti normativi; ▪ collaborare con il team di risposta agli incidenti per valutare l'efficacia organizzativa agli eventi di sicurezza e contribuire all'aggiornamento della policy in base all'esperienza acquisita.
Digital Transformation Management	Assicurare che la Security Awareness Policy sia implementata in modo efficace attraverso l'utilizzo di tecnologie sicure, informazione appropriata e risposta pronta agli incidenti. In particolare, è responsabile di: ▪ implementare e manutenere le misure di sicurezza tecnologiche, quali firewall, antivirus e aggiornamenti software, per proteggere l'infrastruttura IT dall'accesso non autorizzato e dalle minacce; ▪ far monitorare gli indicatori di sicurezza, inclusi tentativi di accesso non autorizzato, anomalie nel traffico di rete e altri comportamenti sospetti, per identificare e rispondere prontamente alle minacce; ▪ assicurare che le politiche di sicurezza dell'informazione siano implementate a livello tecnologico, ad esempio attraverso la configurazione sicura di dispositivi e reti, l'applicazione di controlli di accesso e la gestione delle autorizzazioni; ▪ collaborare con altre funzioni aziendali, come Internal Audit & Compliance, per garantire che le iniziative di consapevolezza della sicurezza siano conformi ai requisiti normativi e alle migliori pratiche del settore; ▪ partecipare alla risposta agli incidenti di sicurezza informatica, fornendo supporto tecnico per identificare, contenere e risolvere le violazioni della sicurezza; ▪ monitorare costantemente il panorama delle minacce e definire un efficace processo di *patch management* coordinandolo e

	contribuendo all'aggiornamento continuo delle politiche e delle procedure di sicurezza in base alle nuove sfide e alle nuove tecnologie emergenti.
Human Resources & Organization (HR&O)	▪ Educare e sensibilizzare i dipendenti riguardo alle minacce alla sicurezza informatica e per promuovere comportamenti sicuri, attraverso l'implementazione di programmi di formazione sulla sicurezza; ▪ collaborare, in caso di violazioni della sicurezza o incidenti informatici, con la funzione Digital Transformation Management per gestire la risposta agli incidenti. Questo potrebbe includere la comunicazione con i dipendenti, la gestione delle conseguenze disciplinari (se necessario) e l'aggiornamento delle politiche di sicurezza; ▪ integrare le politiche di sicurezza nelle politiche del personale.
Corporate Communication (CC)	Mantenere una comunicazione continua riguardo alle minacce alla sicurezza informatica e alle best practice. Questo può includere la pubblicazione di notizie su intranet, l'organizzazione di sessioni informative e la realizzazione e distribuzione di risorse educative digitali.
Chief Information Security Officer (CISO)	▪ Definire, implementare, comunicare e mantenere nel tempo obiettivi, requisiti, strategie e politiche di sicurezza informatica, in linea con gli obiettivi strategici dell'azienda. Assicurare risorse e una corretta allocazione del budget in coordinamento con il Chief Strategy & Transformation Officer e con l'alta Direzione aziendale, per implementare la strategia di sicurezza informatica; ▪ implementare politiche e procedure aziendali nel rispetto di Regolamenti, Leggi e standard internazionali in materia di sicurezza delle informazioni; ▪ contribuire alla progettazione, implementazione e supervisione della corretta applicazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), e contribuirne al miglioramento continuo;

	▪ sviluppare piani di sicurezza informatica, garantendo la resilienza dell'organizzazione agli incidenti informatici; ▪ identificare rischi legati alla sicurezza informatica, in modo che siano opportunamente indirizzati e trattati dalle funzioni aziendali coinvolte; ▪ in caso di incidenti di sicurezza informatica, contribuire alla risoluzione dei problemi individuati; ▪ sviluppare relazioni con autorità e comunità legate alla sicurezza informatica; ▪ influire sulla cultura della sicurezza informatica dell'organizzazione, educando e informando sui rischi e le minacce alla sicurezza informatica e sul loro impatto sull'organizzazione stessa.
Dipendenti e collaboratori	▪ Partecipare alle attività di formazione sulla sicurezza dell'informazione; ▪ aderire alle politiche e alle procedure correlate adottando dei comportamenti idonei nell'utilizzo delle risorse informatiche.
Security Operation Center (SOC)	▪ Progettare e garantire il costante aggiornamento ed evoluzione tecnologica di una architettura di supervisione, controllo e monitoraggio di tutti gli eventi rilevanti in merito alla sicurezza; ▪ eseguire il monitoraggio continuativo degli indicatori di sicurezza, inclusi tentativi di accesso non autorizzato, esposizione del parco installato ai CVE noti, anomalie nel traffico di rete, e altri comportamenti sospetti, per identificare e rispondere prontamente alle minacce; ▪ definire ed attuare in conformità ad un processo ben definito in termini di procedure, ruoli, e responsabilità per la rilevazione degli incidenti informatici e per l'attuazione della immediata risposta in collaborazione con il fornitore esterno che opera sulle risorse e tutti gli altri enti che concorrono alla opportuna gestione dell'incidente; ▪ produrre una reportistica periodica relativa alle anomalie rilevate, opportunamente classificate per livello di rischio associato; ▪ produrre e fornire richieste di intervento, raccomandazioni di modifica e/o aggiornamento della configurazione di dispositivi, applicazioni e reti, all'ente

	aziendale preposto alla gestione degli stessi laddove l'analisi delle rilevazioni di monitoraggio inducano azioni correttive o di miglioramento.

5. Formazione e sensibilizzazione

Italtel, al fine di consolidare il mindset orientato alla security awareness in tutta l'organizzazione, si impegna a sensibilizzare e educare circa i diversi temi relativi alla sicurezza delle informazioni, tutti i dipendenti delle sedi italiane. La formazione e la continua informazione sono infatti azioni considerate fondamentali, previste nell'ambito del *Security Awareness Program* di Italtel. In particolare:

- Fornisce formazione inziale a tutti i nuovi assunti e periodica (almeno una volta l'anno) a tutti i dipendenti e, se necessario, a terze parti. Tale formazione è finalizzata al riconoscimento di potenziali minacce, come phishing, malware e attacchi con tecniche di social engineering, etc.

- Mantiene costantemente informato tutto il personale, attraverso diverse modalità e azioni di comunicazione (e-mail, news sulla intranet, webinar, etc.), promosse dalle funzioni *Corporate Communication/Human Resources & Organization*, circa:
  - Politiche e procedure di sicurezza, comprese le procedure di accesso e di gestione delle password.
  - Uso consapevole delle risorse, promuovendo pratiche sicure nell'uso di dispositivi, reti e dati aziendali.

Sono condotte, inoltre, valutazioni periodiche della consapevolezza della sicurezza attraverso test, esercitazioni e feedback per garantire il miglioramento continuo.

6. Adozione di comportamenti responsabili

La sicurezza delle informazioni è una responsabilità collettiva. Pertanto, tutti coloro ai quali è rivolta la presente policy, hanno il dovere etico e professionale di adottare comportamenti responsabili, in sintonia con la presente policy, per garantire la sicurezza delle informazioni aziendali anche al di fuori dell'ambiente tradizionale dell'ufficio.

In particolare, durante il lavoro remoto, ogni dipendente è tenuto ad applicare quanto disposto dalla presente policy e, in particolare:

- Proteggere le informazioni sensibili e aziendali con la stessa diligenza e attenzione riservate alle attività presso le sedi aziendali.
- Non condividere informazioni aziendali con persone non autorizzate e mantenere la confidenzialità delle informazioni.
- Segnalare immediatamente qualsiasi possibile violazione della sicurezza.
- Utilizzare solo dispositivi aziendali approvati e assicurarsi che essi siano adeguatamente protetti con software antivirus aggiornati e password robuste.
- Evitare l'uso di reti Wi-Fi pubbliche non sicure e adottare misure di sicurezza come l'utilizzo di connessioni VPN aziendali per proteggere la trasmissione di dati.

7. Linee guida per la sicurezza delle informazioni

Si riportano di seguito le regole da applicare per proteggere le informazioni e garantire la sicurezza dei sistemi informativi e, in generale, delle risorse informatiche, opportunamente approfondite nelle relative policy e procedure richiamate al paragrafo 3. della presente policy.

Per completezza, si rimanda al documento “Disposizioni per il corretto utilizzo delle risorse informatiche aziendali”.

7.1. Accesso alle risorse informatiche

L'accesso alle risorse informatiche dell'organizzazione avviene mediante l’uso di credenziali univoche (id utente e password), assegnate individualmente. Ciascuno assegnatario è responsabile di tutte le azioni condotte sui sistemi IT di Italtel tramite l’utilizzo delle proprie credenziali.

In caso di sospetta violazione delle credenziali utente, è necessario fornire tempestiva comunicazione al Security Operation Center (SOC)di Italtel al numero +390243880089.

7.2. Gestione delle password

Gli utenti sono tenuti a seguire le linee guida per la creazione e la gestione sicura delle password, di cui al documento “Gestione delle password”.

È vietato:

- divulgare, cedere o condividere le proprie credenziali di accesso;
- stampare, memorizzare nel proprio PC o in rete le proprie credenziali;
- lasciare incustodite copie delle proprie credenziali.

7.3. Sicurezza dei dispositivi mobili

I dispositivi mobili aziendali (laptop, telefoni cellulari, tablet…) sono protetti con password e crittografia.

I dispositivi mobili di archiviazione (come chiavette USB, CD, DVD e dischi rigidi rimovibili) non possono essere utilizzati salvo nei casi di esplicita autorizzazione da parte dell’azienda.

7.4. Installazioni software

Gli utenti non possono installare software diversi da quelli ricevuti in dotazione dalla Società, salvo in caso di autorizzazione esplicita.

7.5. Aggiornamenti software

Tutti gli utenti devono assicurarsi che i software installati sui dispositivi a loro assegnati e il software antivirus siano aggiornati.

In particolare, gli utenti non devono posporre le installazioni degli aggiornamenti proposti e devono assicurarsi che il software antivirus sia correttamente funzionante e aggiornato.

Gli utenti sono tenuti a segnalare al Service Desk aziendale eventuali casi di fallimento della procedura di aggiornamento dei software installati.

7.6. Sicurezza dei dati

Gli utenti devono adottare tutte le misure necessarie a salvaguardare la confidenzialità, l’integrità e la disponibilità dei dati aziendali.

7.7. Utilizzo di Internet e posta elettronica

Si richiama l’attenzione ad un utilizzo sicuro di Internet e della posta elettronica al fine di evitare l’ingresso e la diffusione in azienda di software malevoli.

7.8. Segnalazione degli incidenti di sicurezza

Gli utenti devono segnalare qualsiasi incidente di sicurezza o attività sospetta al Security Operation Center (SOC) di Italtel al numero +390243880089

La tempestiva segnalazione è essenziale per limitare potenziali danni.

8. Monitoraggio e aggiornamento continuo

Il CISO si riserva il diritto di monitorare l'uso delle risorse informatiche per garantire la conformità a questa policy, che sarà riesaminata e aggiornata periodicamente per riflettere le migliori pratiche di sicurezza in risposta a nuove minacce.

9. Violazioni delle regole di sicurezza

L'inosservanza delle regole di sicurezza può dar luogo all'applicazione di provvedimenti disciplinari previsti dalla contrattazione collettiva di lavoro e dal contratto di riferimento, nonché delle eventuali conseguenze in tema di responsabilità civile e/o penale delle azioni civili e penali stabilite dalla legge. Nel caso di soggetti esterni, alla risoluzione del rapporto contrattuale in essere e a sanzioni civili e/o penali.

Italtel S.p.A.
Benedetto Di Salvo
Chief Executive Officer