T communication s.r.l.
Politica di sicurezza ITC
IS08

Introduzione

T communication s.r.l. (di seguito, T communication) riconosce che i sistemi e le informazioni ITC sono beni essenziali per sostenere gli obiettivi strategici della T communication. T communication riconosce i propri obblighi di proteggere le informazioni dalle minacce interne ed esterne e riconosce che una gestione efficace della sicurezza delle informazioni è fondamentale per garantire l'abilitazione delle ITC e l'erogazione di funzioni e servizi aziendali. T communication si impegna a preservare la riservatezza, l'integrità e la disponibilità di tutti i beni materiali ed elettronici.

La gestione della sicurezza delle informazioni è un ciclo continuo di attività volto al miglioramento continuo in risposta a minacce e vulnerabilità emergenti e mutevoli. Può essere definito come il processo di protezione delle informazioni dall'accesso, divulgazione, modifica o distruzione non autorizzati ed è vitale per la protezione delle informazioni e della reputazione di T communication.

Questa politica descrive in dettaglio l'approccio di T communication alla gestione della sicurezza delle tecnologie dell'informazione e della comunicazione (ICT), che non contiene informazioni sensibili o riservate e può essere pubblicizzata liberamente alle parti interessate. Una versione aggiornata di questo documento è disponibile per il personale di T communication sulla intranet aziendale ed è disponibile per le parti esterne sul sito web di T communication all'indirizzo www.T communication.it

L'approccio si basa sulle raccomandazioni contenute nella norma ISO27002, un codice di condotta per la gestione della sicurezza dell'informazione.

1. Campo di applicazione

La presente politica di sicurezza ITC si applica a:

- Sistemi ICT appartenenti a, o sotto il controllo di, T communication;
- Informazioni memorizzate o in uso su T communication;
- Tutte le parti che hanno accesso a, o utilizzano, sistemi ICT e informazioni appartenenti a, o sotto il controllo di, T communication , inclusi:
  - Dipendenti della società
  - Collaboratori
  - Fornitori
  - Partner e Clienti
  - Qualsiasi altra parte che utilizzi le risorse ICT di T communication.

L'applicazione di questa politica si applica a tutto il ciclo di vita delle informazioni, dall'acquisizione alla creazione, fino all'utilizzo ed allo stoccaggio.

2. Dichiarazione politica

La politica di sicurezza dell'informazione si basa sui principi stabiliti nelle linee guida per la sicurezza dell'informazione (*ISO/IEC 27002).*
T communication è impegnata nello sviluppo e nella manutenzione di un sistema di gestione della sicurezza delle informazioni basato sullo standard internazionale. T communication ha sviluppato questa politica di sicurezza ITC per:

- Fornire un quadro che consenta di mantenere la riservatezza, l'integrità e la disponibilità delle risorse ITC.
- Ottimizzare la gestione dei rischi prevenendo e minimizzando l'impatto degli incidenti di sicurezza ICT;
- Garantire che tutte le violazioni della sicurezza ITC siano segnalate, esaminate e, se necessario, adottate misure adeguate;
- Garantire che i requisiti di sicurezza delle informazioni ITC siano comunicati regolarmente a tutte le parti interessate e periodicamente monitorati.

Uso autorizzato

L'accesso ai sistemi e alle informazioni ITC di cui è responsabile T communication è consentito a sostegno delle attività commerciali di T communication svlte per conto delle società terze Clienti. Gli utenti autorizzati sono definiti come: dipendenti, collaboratori, fornitori, personale anche temporaneo, partner e clienti nell'utilizzo dei servizi di informazione forniti da T communication.

Consapevolezza della sicurezza

T communication si impegna a promuovere pratiche di lavoro sicure. Tutti i dipendenti riceveranno una formazione di sensibilizzazione alla sicurezza commisurata alla classificazione delle informazioni e dei sistemi a cui hanno accesso. Il personale che svolge ruoli specialistici ITC riceverà una formazione adeguata in relazione al suo ruolo. È responsabilità dei dipendenti assicurarsi di essere adeguatamente informati sulle politiche e procedure di sicurezza dell'informazione.

Continuità operativa

T communication ha sviluppato e mantiene una strategia di continuità operativa basata su una valutazione specifica del rischio per mantenere funzioni aziendali critiche in caso di interruzione significativa dei servizi o degli impianti sui quali T communication fa affidamento.

Monitoraggio e relazioni

T communication si riserva il diritto di monitorare l'utilizzo di sistemi e informazioni ICT, incluso l'utilizzo di e-mail e Internet, per proteggere la riservatezza, l'integrità e la disponibilità delle risorse informative di T communication e garantire la conformità con le politiche di T communication; questo monitoraggio avviene anche attraverso l'aggiornamento dei documenti di nomina dei propri dipendenti e collaboratori ad autorizzazi al trattamento dei dati personali ed aziendali (cfr. nomina autorizzato secondo il Regolamento UE 2016/679). Come parte del processo di revisione, l'Internal Audit valuterà regolarmente la conformità con la Politica di Sicurezza ICT di T communication e con i controlli ISO 27001 applicabili e riferirà le questioni alla Direzione, ove opportuno. Gli incidenti di sicurezza segnalati attraverso la Politica e le Procedure di Gestione degli Incidenti di Sicurezza, informeranno sull'efficacia dei controlli ISO 27001 e contribuiranno a identificare i requisiti e i miglioramenti di formazione e sensibilizzazione attraverso la Procedura di Miglioramento.

Valutazione del rischio

T communication ha sviluppato una strategia di gestione del rischio e il rischio per i sistemi ITC e le informazioni di T communication sarà gestito nell'ambito di questo quadro con riferimento alle linee guida dettagliate nella ***norma ISO/IEC 27005:2018 Tecnologia dell'informazione. Tecniche di sicurezza Gestione dei rischi per la sicurezza dell'informazione.*** Le revisioni sono indipendenti, imparziali e verificate sia dall'audit interno che da parti esterne, quando richiesto.

Revisione della politica di sicurezza

T communication effettuerà una revisione annuale della politica o a seguito di incidenti significativi per la sicurezza, di modifiche alla legislazione italiana o dell'UE o di modifiche al requisito o alla struttura aziendale di T communication.

Sanzioni

Il mancato rispetto da parte dei dipendenti di T communication della Politica di sicurezza delle informazioni di T communication può portare a un'azione disciplinare nell'ambito del procedimento disciplinare di T communication.
Il mancato rispetto della politica di sicurezza delle informazioni di T communication da parte di clienti, parter, fornitori, dipendenti, collaboratori, personale anche temporaneo, può comportare la risoluzione dei contratti e dei collegamenti, la sospensione dei servizi e/o l'avvio di procedimenti giudiziari.

3. Adempimenti di obblighi legali e contrattuali

T communication si atterrà a tutta la legislazione italiana relativa alla memorizzazione e all'elaborazione delle informazioni, inclusi il Regolamento Ue 2016/679 ed il D.lgs 101/2018.
T communication si conformerà inoltre a tutti i requisiti, standard e principi contrattuali richiesti per mantenere le funzioni aziendali di T communication, tra cui:

- Tutela dei diritti di proprietà intellettuale;
- Protezione dei dati di T communication anche secondo i vincoli di riservatezza contrattualmente stabiliti volta per volta;
- Controllo di conformità e procedure di audit;
- Prevenzione dell'uso improprio dei sistemi informatici (asset).

4. Responsabilità

Coordinamento: T communication coordina la gestione della sicurezza delle informazioni sulla rete aziendale attraverso il Reparto IT.

Responsabile della sicurezza: l'Ufficio IT di T communication è responsabile di assicurare che le politiche e le procedure siano in atto per coprire tutti gli aspetti dei sistemi ICT e della sicurezza delle informazioni. Tutte le politiche saranno comunicate attraverso T communication per garantire buone pratiche di lavoro e ridurre al minimo il rischio per la reputazione di T communication.

Direzione aziendale: ha la responsabilità di garantire che i sistemi e le informazioni ITC siano gestiti in conformità con la politica di sicurezza ITC di T communication. La responsabilità quotidiana della gestione dei sistemi ITC e delle informazioni può essere delegata al personale addetto alla gestione delle informazioni.

Utenti delle risorse: È responsabilità di ogni persona o ente anche terzo che ha accesso ai sistemi e alle informazioni ITC di T communication conformarsi alla politica di sicurezza ITC di T communication, alle linee guida e alle procedure associate e adottare misure adeguate per salvaguardare la sicurezza dei sistemi ITC e delle informazioni a cui ha accesso. Qualsiasi sospetto o effettivo punto debole, minaccia, evento o incidente in materia di sicurezza deve essere immediatamente segnalato al Reparto IT ed alla Direzione.

5. Elaborazione di politiche , procedure e orientamenti specifici in materia di ITC

T communication valuterà annualmente la necessità di revisione delle proprie politiche , procedure e linee guida ICT per gestire il rischio di minacce emergenti ai suoi sistemi e servizi. Questo lavoro sarà coordinato dal Reparto IT. Un elenco dei documenti giustificativi attuali figura nelle appendici A-B. Le nuove politiche e procedure sono distribuite a tutti i soci di T communication s.r.l. al momento dell'emissione. Le appendici A-B della presente politica sono aggiornate nel corso dell'esame annuale della sicurezza ITC.

6. Violazioni della Politica

Le violazioni della presente politica e/o gli incidenti di sicurezza possono essere definiti come eventi che potrebbero avere, o hanno avuto come conseguenza, perdite o danni alle attività di T communication, o come eventi che violano le procedure e le politiche di sicurezza di T communication.

I dipendenti, collaboratori, clienti, partner e fornitori di T communication hanno la responsabilità di segnalare gli incidenti di sicurezza e le violazioni di questa politica il più rapidamente possibile attraverso la Procedura di segnalazione degli incidenti di T communication (procedura IS20). Tale obbligo si estende anche a qualsiasi organizzazione esterna incaricata di supportare o accedere ai sistemi informativi di T communication.

T communication adotterà misure appropriate per porre rimedio a qualsiasi violazione della politica e delle relative procedure e linee guida attraverso i relativi quadri normativi in vigore. Nel caso di una persona, la questione può essere trattata nell'ambito del procedimento disciplinare.

7. Documentazione e registri associati

Nome documento/registrazione	Posizione di stoccaggio	Proprietario	Controllo della protezione	Programma di ritenzione
Tutte le politiche e procedure in materia di ITC	Ufficio IT	RSGSI	Controllato: Accesso protetto da password	1 anno

8. Gestione Documentale

Il presente documento è valido a partire dal 23/11/2020

Il presente documento viene periodicamente e comunque con cadenza almeno annuale al fine di garantire il rispetto dei seguenti criteri previsti.

- Conformità ai requisiti della norma ISO 27001:2013
- Requisiti legislativi definiti dalla legge, e in particolare dal Regolamento UE 2016/679.

Appendice A: Elenco delle politiche di sicurezza ISMS

Titolo	Stato	Data recensione
IS01 Dichiarazione di applicabilità	Pubblicato	23/11/2020
Is02 Politica d'uso accettabile	Pubblicato	23/11/2020
IS03 Politica di controllo degli accessi	Pubblicato	23/11/2020
IS04 Politica di gestione patrimoniale	Pubblicato	23/11/2020
IS05 Politica di gestione delle registrazioni	Pubblicato	23/11/2020
IS06 Politica di formazione	Pubblicato	23/11/2020
IS 07 Criteri di crittografia	Pubblicato	23/11/2020
IS 08 Politica di sicurezza ITC	Pubblicato	23/11/2020
IS10 Politica backup e ripristino delle informazioni	Pubblicato	23/11/2020
IS 13 Politica ISGS	Pubblicato	23/11/2020
IS 14 Gestione operative	Pubblicato	23/11/2020
IS 17 Criteri di scansione e smaltimento	Pubblicato	23/11/2020
IS 21 Criteri di sicurezza server	Pubblicato	23/11/2020
IS 24 Politica di rete wireless	Pubblicato	23/11/2020

Appendice B: Elenco delle procedure di sicurezza ISMS

Titolo	Stato	Data recensione
IS29 Piano di continuità operativa per le ITC	Pubblicato	23/11/2020
IS30 Procedura di non conformità, azioni correttive e preventive	Pubblicato	23/11/2020
IS31 Procedura di segnalazione e gestione degli incidenti	Pubblicato	23/11/2020
IS33 Procedure di sviluppo e manutenzione dei sistemi informatici	Pubblicato	23/11/2020
IS34 Procedura di audit interno ISMS	Pubblicato	23/11/2020
IS36 Procedura per software dannoso e antivirus	Pubblicato	23/11/2020
IS38 Procedura per le infrastrutture fisiche e ambientali	Pubblicato	23/11/2020
IS42 Procedure di telelavoro e di lavoro mobile	Pubblicato	23/11/2020