INFORMATION SECURITY AND PRIVACY POLICY

Redazione	Responsabile SGSI, Privacy Officer
Convalida	CISO, Responsabile Risk, Compliance, Quality & Anti-Corruption
Approvazione	Risk Owner

Rev.	*Data*	*Descrizione*
01	01/07/2024	Prima emissione
02	10/10/2024	Armonizzazione della Policy in ottica SGI
03	23/05/2025	Revisione annuale per ulteriore armonizzazione e allineamento alla Comunicazione di Servizio 02/2025
04	04/04/2025	Revisione per integrazione requisiti ISO/IEC 27701:2019

Indice

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente documento di Policy per la Sicurezza e la Privacy delle Informazioni è stato predisposto nel rispetto dei requisiti della Norma ISO/IEC 27001:2022 e ISO/IEC 27701:2019 e rappresenta il quadro di riferimento dei principi, delle linee guida e delle regole che devono essere adottate per la sicurezza delle informazioni TINEXTA CYBER S.p.A. (di seguito, anche TINEXTA CYBER).

I principi, le linee guida e le regole sono di natura generale, sono dedicate ai vari aspetti della sicurezza delle informazioni e sono articolate secondo la struttura suggerita dall'Annex A della Norma ISO 27001, dagli Annex A/B della norma ISO 27701 e dagli standard e best practices ad essa correlati.

Finalità specifiche del presente documento sono:

- Stabilire la normativa generale e i principi base per il corretto trattamento e tutela delle informazioni e dei beni informatici, dell'Azienda e dei Clienti;
- Adempiere agli obblighi imposti dalle leggi in tema di sicurezza delle informazioni;
- Fornire una base comune di linee guida e regole per lo sviluppo e l'attuazione delle procedure operative per la gestione della sicurezza delle informazioni;
- Definire ruoli e responsabilità, generali e specifiche, per tutti gli aspetti legati alla sicurezza delle informazioni e dei beni informatici, dell'Azienda e dei Clienti;
- Assicurare il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni di TINEXTA CYBER, inteso come obiettivo fondamentale dei sistemi di gestione che il Management e tutti i dipendenti devono contribuire a raggiungere.

La ***Information Security and Privacy Policy*** è destinata ai dipendenti TINEXTA CYBER ed a tutti gli stakeholders interessati (Clienti, Fornitori e altre terze parti). L'ambito di applicazione della Information Security and Privacy Policy coincide con il perimetro del Sistema di Gestione per la Sicurezza Informazioni (SGSPI) implementato sul contesto dell'Organizzazione. La rivisitazione del presente documento è prevista con cadenza almeno annuale e, comunque, in occasione di variazioni significative di elementi che hanno impatti sul SGSPI e sulla sicurezza delle informazioni in azienda al fine di garantirne l'adeguatezza al contesto.

2. RUOLI E RESPONSABILITÀ PER LA SICUREZZA INFORMAZIONI

La Direzione Generale TINEXTA CYBER, in relazione alla struttura organizzativa aziendale e alle dimensioni interfunzionali della sicurezza delle informazioni, ha individuato i seguenti ruoli ed organi per la gestione del SGSPI:

- Risk Owner;
- CISO;
- Responsabile Sistema Gestione Sicurezza Informazioni (anche "Responsabile SGSI"), supportato dal Referente Sicurezza Fisica e dal Referente Sicurezza Logica;
- Responsabile Risk, Compliance, Quality & Anti-Corruption;
- Data Protection Officer (anche "DPO");
- Privacy Officer;
- Comitato IS.

3. LINEA GUIDA: SICUREZZA NEI COMPORTAMENTI DEL PERSONALE

Tutti i dipendenti, nonché i collaboratori e le terze parti, sono responsabili della tutela delle informazioni TINEXTA CYBER e della strumentazione informatica di TINEXTA CYBER ad essi affidata.

I dipendenti, i collaboratori e le terze parti devono applicare le policies, le regole e le procedure aziendali in tema di sicurezza delle informazioni, per quanto di rispettiva competenza.

Il management di TINEXTA CYBER si impegna inoltre a:

- Richiedere il rispetto delle policies, delle regole e delle procedure del SGSPI da parte dei dipendenti, dei collaboratori e delle terze parti coinvolte;
- Favorire in azienda la diffusione della cultura della sicurezza delle informazioni mediante la conoscenza e l'adozione della presente policy e di tutte le regole del SGSPI da parte dei dipendenti, dei collaboratori e delle terze parti coinvolte;
- Supportare gli organi di gestione del SGSPI nelle fasi di valutazione dei rischi e individuazione di soluzioni adeguate nella propria area di competenza;
- Attuare, nel rispetto dell'ambito di propria competenza, le azioni di mitigazione del rischio approvate nel rispetto della pianificazione definita.

4. CLASSIFICAZIONE E PROTEZIONE DELLE INFORMAZIONI

TINEXTA CYBER adotta la classificazione delle informazioni, soprattutto dei documenti sia elettronici che cartacei, presenti in azienda in base alla loro criticità. Il trattamento di tali informazioni deve avvenire in coerenza con le modalità definite per ciascuno dei livelli riportati in questa policy. La classificazione di tutte le pagine dei documenti prodotti internamente è effettuata dall'autore apponendo relativa etichetta del livello di classificazione. I livelli di classificazione adottati in TINEXTA CYBER sono:

Livello	Permission	Descrizione	Esempi	Modalità di gestione
Riservato	Soci della Società, membri degli Organi Amministrativi della Società (Consiglio di Amministrazione, Collegio Sindacale), Procuratori, Organismo di Vigilanza, Società di Revisione	Documenti e informazioni altamente critici che, se noti a persone diverse da quelle autorizzate a conoscerle, potrebbero danneggiare gravemente l'Azienda ed i suoi interessi. Informazioni di tale tipo sono tipicamente quelle legate direttamente al business e alle scelte strategiche	▪ Progetti d'investimento, accordi tra società, etc. Informazioni riservate la cui diffusione può portare ad azioni legali e/o a sanzioni penali	▪ L'accesso da parte di altri soggetti, interni o esterni all'Azienda, deve essere autorizzato dall'owner del documento, a meno che non sia diversamente specificato all'interno dello stesso documento; ▪ le copie cartacee ed i supporti elettronici removibili in cui sono conservati non devono essere mai lasciati

		dell'Azienda ovvero documenti di carattere prettamente tecnico / infrastrutturale / applicativo. La loro diffusione, sia essa dolosa o accidentale, può avere, ad esempio, conseguenze economiche, legali, di immagine o può mettere a repentaglio operazioni commerciali o trattative contrattuali.		incustoditi senza adeguate protezioni; in particolare, le copie cartacee devono essere riposte in armadi chiusi a chiave quando non più necessarie; ▪ deve essere prevenuta la creazione di copie cartacee ed elettroniche, in particolare su memorie esterne, non strettamente necessarie; ▪ quando necessario stampare i documenti, le copie devono essere prelevate immediatamente dalle stampanti; in particolare da quelle accessibili a più persone; ▪ deve essere posta particolare attenzione alla profilazione di utenze di sistemi informatici contenenti tali tipi di dati; ▪ l'elaborazione delle informazioni elettroniche deve avvenire su architetture di rete logico/fisiche sicure come VLAN dedicate controllate da uno o più livelli di firewall; ▪ la comunicazione deve avvenire mediante utilizzo

				di canali sicuri come VPN, linee dedicate o soluzioni equivalenti; ▪ le copie elettroniche su supporti removibili devono essere crittografate; ▪ le copie cartacee non più necessarie devono essere scrupolosamente distrutte; ▪ l'invio di copie cartacee deve avvenire in busta chiusa. In caso di diffusione delle informazioni, avvenuta o sospettata, deve essere data comunicazione all'owner del documento e al Responsabile SGSI. In caso di impatto su dati personali, la comunicazione deve avvenire anche verso il Privacy Officer.
Confidenziale	Ruoli aziendali / persone specificamente individuati	Documenti e informazioni legati tipicamente all'operatività ordinaria dell'Azienda che possono essere noti esclusivamente ad alcuni ruoli/persone in relazione alle proprie attività.	▪ Piani strategici, piani commerciali, etc. ▪ Documenti riportanti dati personali comuni e particolari ▪ Dati patrimoniali aziendali ▪ Contratti con clienti, trattative contrattuali, etc. ▪ Contratti con fornitori, trattative contrattuali, etc. ▪ Accordi di partnership ▪ Costi del personale aziendale	▪ L'accesso da parte di altri soggetti, interni o esterni all'Azienda, deve essere autorizzato dall'owner del documento, a meno che non sia diversamente specificato all'interno dello stesso documento; ▪ le copie cartacee e i supporti elettronici removibili in cui sono conservati devono essere

			▪ Pratiche di sinistri Codice software coperto da proprietà intellettuale	custoditi in ambienti sicuri; ▪ le copie cartacee devono essere riposte in armadi chiusi a chiave quando non più necessarie; ▪ le copie elettroniche su supporti removibili devono essere crittografate; ▪ l'elaborazione delle informazioni elettroniche deve avvenire su architetture di rete logico/fisiche sicure come VLAN dedicate controllate da uno o più livelli di firewall; ▪ la comunicazione deve avvenire mediante utilizzo di canali sicuri come VPN, linee dedicate o soluzioni equivalenti; ▪ le copie cartacee non più necessarie devono essere distrutte; ▪ l'invio di copie cartacee deve avvenire in busta chiusa. In caso di diffusione delle informazioni, avvenuta o sospettata, deve essere data comunicazione all'owner del documento e al Responsabile SGSI. In caso di impatto su dati personali, la

				comunicazione deve avvenire anche verso il Privacy Officer. Raccolta/Utilizzo di più documenti confidenziali: la necessità di una raccolta di documenti confidenziali presso la stessa sede/ufficio può comportare l'obbligo di rivederne la classificazione, determinare l'eventuale riclassificazione di singoli documenti come strettamente confidenziali e/o richiedere l'introduzione di ulteriori misure di sicurezza per rendere idonea la sede/ufficio se: ▪ complessivamente, la molteplicità dei suddetti documenti è tale da recare un danno grave all'Organizzazione qualora venissero dispersi; ▪ quando i suddetti molteplici documenti, utilizzati con altre combinazioni di dati (ad esempio, nome e indirizzo), potrebbero diventare oggetto di attacco in ragione dell'elevata criticità;

				▪ quando in un sistema sono presenti molteplici registrazioni di estremi bancari che potrebbero diventare oggetto di attacco alla stregua dell'ipotesi precedentemente decritta. In caso di dubbi circa le informazioni in proprio possesso, l'utente deve sempre rivolgersi al referente aziendale individuato.
Interno	Tutti i dipendenti della Società	Documenti e informazioni che possono essere acceduti da tutti i dipendenti dell'Azienda.	▪ Documentazione dei Sistemi di Gestione dei processi aziendali ▪ Regolamenti aziendali Documentazione di progetti ordinari ▪ Comunicazioni aziendali interne destinate a tutto il personale Documenti tecnica di prodotto/servizio	▪ L'accesso da parte di soggetti esterni all'Azienda deve essere autorizzato dall'owner del documento, a meno che non sia diversamente specificato all'interno dello stesso documento; ▪ le copie cartacee non devono essere lasciate in vista al di fuori degli orari di lavoro; ▪ l'accesso da parte di terzi ai sistemi informatici contenenti tali dati deve essere consentito soltanto se autorizzati; ▪ l'elaborazione delle informazioni elettroniche deve avvenire su architetture di rete logico/fisiche sicure come VLAN dedicate controllate da uno

				o più livelli di firewall; ▪ la comunicazione deve avvenire mediante utilizzo di canali sicuri come VPN, linee dedicate o soluzioni equivalenti. In caso di diffusione delle informazioni, avvenuta o sospettata, deve essere data comunicazione all'owner del documento e al Responsabile SGSI. In caso di impatto su dati personali, la comunicazione deve avvenire anche verso il Privacy Officer.
Pubblico	Anche gli esterni alla Società	Documenti e informazioni che possono essere accedute liberamente anche da persone esterne all'Azienda.	▪ Dati contabili e di bilancio da comunicare all'esterno ▪ Comunicati stampa e annunci ufficiali Materiale pubblicitario e divulgativo	Non sono previste particolari accortezze per la gestione di tali tipi di documenti e delle informazioni ivi contenute.

5. LINEA GUIDA: SICUREZZA FISICA

Sono individuate ed applicate specifiche ed adeguate misure per garantire la sicurezza fisica, tra cui:

- Controllo fisico accessi (es. badge, registro ingressi, controllo passo carrabile, etc.);
- Sistemi antintrusione (es. sensori volumetrici, sensori perimetrali, videosorveglianza, etc.);
- Impianti di alimentazione elettrica (es. cabina elettrica, cablaggi, quadri elettrici, gruppi di continuità, UPS, gruppo elettrogeno, etc.);
- Sistemi antincendio (es. estintori, manichette antincendio, impianti per lo spegnimento automatico, rilevazione dei fumi, ecc.);
- Sistemi antiallagamento.

L'individuazione delle misure da applicare è basata sulla valutazione della criticità delle risorse da proteggere. È assicurata la corretta e periodica manutenzione degli impianti per garantire il loro funzionamento ottimale ed il rispetto delle prescrizioni di legge.

6. LINEA GUIDA: CONTROLLO ACCESSI LOGICI

Sono applicate procedure per controllare la distribuzione dei diritti di accesso ai dispositivi, ai server, ai software e per la gestione degli account utente, in tutte le fasi: dalla creazione dell'account utente, alla sua modifica, aggiornamento, eliminazione.

I diritti di accesso sono definiti in base al ruolo ed alle mansioni svolte dall'utente ed in base alle effettive necessità lavorative (criterio del *need to know*).

I diritti di accesso di tipo Amministrativo sono limitati il più possibile e controllati nel rispetto delle normative vigenti (Provvedimento del Garante della Privacy sugli Amministratori di Sistema).

Le utenze e i profili di accesso sono periodicamente controllati per verificarne l'adeguatezza nel tempo e sanare situazioni non conformi.

La metodologia utilizzata da TINEXTA CYBER per l'autenticazione di ciascun utente è commisurata alla criticità dei dati contenuti nei sistemi, in base a cui deve essere valutata l'opportunità di utilizzo di metodi di autenticazione più vincolanti (*strong authentication*). Di norma viene utilizzata la combinazione di user-id e password.

Ove possibile, deve essere garantita la robustezza delle password mediante il rispetto di criteri di complessità e la sua scadenza periodica.

7. LINEA GUIDA: GESTIONE DEI SISTEMI ICT

Al fine di garantire la gestione in sicurezza di tutti i sistemi e infrastrutture ICT aziendali, è necessario che siano adeguatamente documentate le procedure operative e che siano chiaramente definite le responsabilità in merito a:

- Installazione del software nei server e nei desktop/notebook;
- Adeguamento della capacità delle risorse ICT;
- Gestione delle vulnerabilità tecniche e relative patch;
- Backup dei sistemi;
- Raccolta e protezione dei log;
- Gestione delle comunicazioni elettroniche e cartacee;
- Trasmissione dei dati;
- Crittografia.

8. LINEA GUIDA: SVILUPPO E MANUTENZIONE SOFTWARE

I processi di sviluppo e manutenzione del software applicativo devono essere opportunamente regolamentati, documentati e gestiti, non solo nell'intento di perseguire la massima qualità di servizio, efficacia ed efficienza operativa, ma anche nell'ottica di garantire che il software rispetti i requisiti di sicurezza necessari. Come descritto al paragrafo precedente, sono state revisionate le "**Tinexta Cyber-Linee guida sullo sviluppo di software sicuro"**, il documento *master* per tutti coloro che si occupano di sviluppo; il documento è diffuso e consultabile online sulla intranet aziendale.

9. LINEA GUIDA: GESTIONE DEGLI INCIDENTI DI SICUREZZA

Gli incidenti devono essere gestiti tempestivamente e appropriatamente, al fine di minimizzare danni ulteriori e di ripristinare al più presto e in modo ottimale le normali condizioni operative. In particolare, è necessario individuare gli incidenti di sicurezza che possono mettere a repentaglio la riservatezza, l'integrità e la disponibilità delle informazioni. Per questo deve essere definito, documentato ed adottato un processo per la gestione degli incidenti che preveda almeno:

- La classificazione degli incidenti in base alla loro priorità;
- La registrazione degli incidenti;
- Opportune modalità di gestione in relazione alla classificazione;
- L'individuazione dei responsabili della risoluzione degli incidenti;
- L'analisi delle problematiche segnalate;
- L'uso di uno strumento per la tracciatura degli incidenti;
- La predisposizione di opportuna reportistica;
- Il riesame periodico degli incidenti principali.

Tutti i dipendenti, i collaboratori e le terze parti sono tenuti a segnalare gli incidenti relativi alla sicurezza delle informazioni TINEXTA CYBER tramite i canali e gli strumenti adottati in azienda.

Qualora l'incidente riguardi i dati personali degli interessati di cui TINEXTA CYBER è Titolare del Trattamento oppure Responsabile esterno del Trattamento, deve essere attivato, ove necessario, il processo di notifica di violazione dati personali al Garante Privacy oppure la comunicazione al Cliente Titolare dei dati coinvolti nella violazione.

10. LINEA GUIDA: GESTIONE DELLA BUSINESS CONTINUITY

TINEXTA CYBER deve adottate strategie e piani per la continuità operativa dei servizi erogati e della sicurezza delle informazioni che tengano conto:

- Dei servizi aziendali valutati critici per il business;
- Dei requisiti minimi di ripristino;
- Dei principali scenari incidentali derivati dalle best practices internazionali;
- Degli impatti dei suddetti scenari sull'azienda e dei conseguenti livelli di rischio.

Il Responsabile SGSI deve assicurare la definizione e l'aggiornamento:

- Dell'elenco dei servizi critici;
- Dei requisiti minimi di ripristino;
- Degli scenari di rischio;
- Degli impatti sull'azienda;
- Delle strategie di ripristino;
- Dei piani e delle procedure di continuità;
- Delle misure che consentono la ripresa del servizio.

Inoltre, il Responsabile SGSI si impegna per garantire:

- La diffusione, all'interno e all'esterno dell'azienda, per quanto necessario, dei piani e delle procedure di continuità;

- L'adeguatezza degli accordi contrattuali con i Fornitori in merito alla gestione (tempi e modi) delle situazioni di disastro, a seconda del loro coinvolgimento nell'erogazione di servizi critici;
- L'esistenza, l'aggiornamento ed il test periodico dei piani di continuità operativa e le relative responsabilità per la gestione della reazione all'incidente e il rispristino del servizio secondo i requisiti minimi definiti, da condividere tra tutte le funzioni coinvolte;
- L'adeguatezza delle soluzioni per la continuità operativa (es. ridondanze dei sistemi, resilienza degli impianti, disponibilità di sedi alternative, distribuzione delle competenze critiche, ecc.).

I requisiti di sicurezza informazioni da applicare nelle situazioni di crisi/disastro (es. autorizzazioni all'accesso dei dati, etc.) sono gli stessi che valgono durante la normale operatività. Analogamente, anche i ruoli e le responsabilità definiti e assegnati per la gestione della sicurezza informazioni durante la normale operatività sono gli stessi che garantiscono la continuità della gestione della sicurezza informazioni anche durante le situazioni di crisi/disastro.

11. LINEA GUIDA: GESTIONE DEI FORNITORI

Il livello di sicurezza garantito dalle terze parti (Fornitori, outsourcers, partners, etc.) deve essere conforme al livello di sicurezza applicato da TINEXTA CYBER, per evitare che i prodotti/servizi acquisiti dall'esterno costituiscano un elemento di debolezza per la sicurezza delle informazioni.

Deve essere fatta preventivamente una valutazione dei rischi delle terze parti e, quindi, devono essere definite e inserite nel contratto le responsabilità, le condizioni specifiche, i requisiti di sicurezza e gli SLA (coerenti con le valutazioni di rischio) che le terze parti sono tenute a rispettare, in particolare nel caso di Fornitori/outsourcers ICT.

Le terze parti, ove applicabile in base alla natura della fornitura, devono assicurare:

- Rispetto delle policy e procedure TINEXTA CYBER relative alla sicurezza delle informazioni;
- Modalità di gestione degli asset TINEXTA CYBER (hardware, software, informazioni) in conformità alle regole aziendali per minimizzare i rischi legati all'accesso da parte di esterni a dati e sistemi TINEXTA CYBER;
- Modalità sicure di trasferimento e di protezione dati e di movimentazione dei supporti di memorizzazione;
- Sensibilizzazione del proprio personale operante in o per TINEXTA CYBER al rispetto della riservatezza dei dati scambiati con TINEXTA CYBER e al rispetto delle linee guida relative al loro trattamento;
- Rispetto della proprietà intellettuale e dei diritti d'autore;
- Rispetto dei requisiti delle leggi e normative in materia di sicurezza e protezione dei dati personali;
- Segnalazione e reporting degli eventuali incidenti di sicurezza che interessano anche TINEXTA CYBER;
- Processi per la gestione di eventuali problemi causati dai difetti dei prodotti/servizi e per la loro soluzione;
- Processi per la gestione di eventuali crisi, predisposizione del BCP, ripristino dei servizi nel rispetto dei requisiti di business continuity TINEXTA CYBER (RTO/RPO), in base agli accordi contrattuali;
- Controllo del rispetto delle condizioni pattuite (es. reportistica, definizione KPI, monitoraggio degli indicatori, ecc.) e rispetto dei tempi di consegna della documentazione di reporting.

Inoltre, le terze parti devono garantire a TINEXTA CYBER che siano da loro applicate analoghe misure di sicurezza delle informazioni verso i sub-Fornitori, in modo da garantire che gli standard di sicurezza richiesti da TINEXTA CYBER siano applicati da tutte le parti coinvolte nella catena di fornitura.

12. LINEA GUIDA: COMPLIANCE E AUDIT

TINEXTA CYBER opera nel rispetto delle leggi nazionali e internazionali applicabili ai settori di mercato per i quali opera, dei regolamenti interni, delle normative volontarie adottate (es. ISO 9001, ISO 27001, ISO 22301 etc.), dei contratti con le controparti esterne. Inoltre, TINEXTA CYBER garantisce l'adeguata disponibilità di documentazione e di risorse per consentire le eventuali attività degli Auditor interni ed esterni.

I principali riferimenti normativi cogenti corrispondono a:

- Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali;
- D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss.mm.ii., per le parti ancora in vigore;
- D.Lgs. 81/2008 "Testo Unico sulla Sicurezza sul Lavoro" e ss.mm.ii.;
- D.Lgs. 231/2001 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" e ss.mm.ii;
- Decreto Legislativo 10 febbraio 2005, n. 30 ("Codice della Proprietà Industriale");
- Direttiva (UE) 2022/2555 (NIS2);
- Regolamento (UE) 2022/2554 (DORA).

Per assicurare il recepimento degli aggiornamenti normativi TINEXTA CYBER si avvale di professionalità esterne esperte. In particolare, il recepimento degli aggiornamenti normativi è controllato dalla Funzione Risk, Compliance, Quality & Anti-Corruption di TINEXTA CYBER (es. normativa privacy, sicurezza sul lavoro, responsabilità amministrativa, ecc.) che assicura i contatti con le Autorità competenti, mentre gli aggiornamenti delle normative di settore (es. norme IVASS, Banca d'Italia, etc.) sono curati dai Responsabili normativi per lo sviluppo software o direttamente dai Clienti che richiedono i necessari aggiornamenti dei processi e delle applicazioni per rispondere ai cambiamenti sopraggiunti.

All'occorrenza, TINEXTA CYBER si serve inoltre di consulenti esterni che supportano l'azienda su tematiche specifiche relative alla normativa di settore.

I Responsabili normativi per lo sviluppo software di TINEXTA CYBER analizzano le implicazioni delle novità normative sull'area di propria pertinenza e ne assicurano l'applicazione per quanto di competenza.