techsystem
Il tuo partner informatico

Information Security Management System – ISO/IEC 27001:2022
Cloud Security – ISO/IEC 27017:2026
PII Protection in Public Cloud – ISO/IEC 27018:2025

Classificazione: C0 — Pubblico

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Techsystem srl
Via Parma 64 Torino (TO)
10153 Torino (TO)
P.IVA 08508960013

Attenzione!

Le informazioni contenute in questo documento e nei suoi allegati sono di esclusiva proprietà di Techsystem srl.
La loro divulgazione a soggetti terzi rispetto ai destinatari è consentita previa autorizzazione esplicita della Direzione aziendale.

techsystem
Il tuo partner informatico

Controllo del documento

Campo	Valore
Codice documento	**ID_520**
Versione	**1.1**
Data di emissione	23/10/2026
Autore / Responsabile	Giuseppe Vacca — g.vacca@techsystem.it
Redazione	Techsystem srl; integra spunti della Politica predisposta dalla consulente nel sistema di gestione consegnato il 19/10/2026 (documento ID_520)
Classificazione	C0 — Pubblico
SGSI di riferimento	ISO/IEC 27001:2022 · ISO/IEC 27017:2026 · ISO/IEC 27018:2025
Requisiti	Clausola 5.2 *(politica per la sicurezza delle informazioni)* · clausole 5.1 e 5.3 *(leadership e ruoli)* · A.5.1 *(politiche per la sicurezza delle informazioni)*
Approvazione	Titolare, in forma elettronica, mediante pubblicazione sul *Portale applicazioni · modulo Presa visione documenti interni* il **23/10/2026**; distribuita a tutto il personale — Titolare, personale tecnico e Amministrazione — con evidenza di presa visione nello stesso modulo
Entrata in vigore	**23/10/2026**
Riesame	annuale dalla data di adozione, e comunque ai cambiamenti significativi (§10)
Collegamento con le registrazioni	PRVIS (presa visione del presente documento)
Cosa cambia rispetto alla versione 1.0	• **Codice** — da D03 a ID_520, secondo l'atto «Codifica dei documenti del Sistema di Gestione» (ID_1158) del 23/10/2026. • **Rimandi** — i documenti citati sono indicati con i codici nuovi. • **Impaginazione** — copertina in prima pagina e, su ogni pagina, piè di pagina con codice, titolo, versione, data e classe (formato dei documenti del SGSI). Il resto del documento è invariato.

1. Scopo

La presente politica esprime l'impegno della Direzione di **Techsystem srl** a proteggere la **riservatezza**, l'**integrità** e la **disponibilità** delle informazioni proprie, dei propri clienti e dei terzi, e stabilisce i principi, gli obiettivi e le responsabilità su cui si fonda il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI). È il documento di riferimento per le politiche per tema e per le procedure del SGSI che la attuano (§9).

2. Campo di applicazione

La politica si applica:

- a **tutto il personale** e ai collaboratori di Techsystem;
- a tutte le **informazioni** trattate da Techsystem, in qualunque forma;
- ai **sistemi e servizi interni**: la sede di Torino, le postazioni, i server, la rete e i servizi cloud in uso;

- ai **servizi erogati ai clienti** con il marchio Smart-IT®, come descritti nel documento *Scopo e campo di applicazione del SGSI* (ID_100);
- allo **sviluppo delle applicazioni interne**; allo sviluppo di software su commessa per i clienti, escluso dal campo di applicazione della certificazione, si applica il versionamento del codice nei repository aziendali.

Il contesto dell'organizzazione e le esigenze e aspettative delle parti interessate sono analizzati nel documento *Contesto e parti interessate* (ID_400), aggiornato almeno una volta l'anno nel riesame della direzione o al mutare dei fattori analizzati.

3. Riferimenti

- ISO/IEC 27001:2022, clausole 5.1, 5.2, 5.3 e controllo A.5.1; ISO/IEC 27017:2026 (servizi cloud); ISO/IEC 27018:2025 (protezione dei dati personali nei servizi cloud).
- Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 196/2003; provvedimento del Garante per la protezione dei dati personali del 27/11/2008 sugli amministratori di sistema.
- *Data Processing Agreement* di Techsystem (ID_1136): obblighi di Techsystem come responsabile del trattamento dei dati personali dei clienti.
- *Scopo e campo di applicazione del SGSI* (ID_100) e *Contesto e parti interessate* (ID_400).

4. Impegni della Direzione

La Direzione si impegna a:

a) verificare che la politica sia **appropriata** alle finalità e al contesto di Techsystem e **compatibile con i suoi indirizzi strategici**;

b) **integrare** i requisiti del SGSI nei processi aziendali;

c) stabilire, attuare, mantenere e **migliorare con continuità** il SGSI;

d) soddisfare i **requisiti applicabili** alla sicurezza delle informazioni: di legge, regolamentari e contrattuali, compresi quelli concordati con i clienti e quelli sulla tutela del software e della proprietà intellettuale;

e) rispettare la normativa sulla **protezione dei dati personali** e gli accordi sul trattamento stipulati con i clienti (ID_1136) per i dati che Techsystem tratta per loro conto, anche nei servizi cloud;

f) **valutare periodicamente i rischi e le opportunità** per la sicurezza delle informazioni, definendo il piano di trattamento e la Dichiarazione di Applicabilità;

g) stabilire **obiettivi di sicurezza misurabili** e riesaminarne il raggiungimento (§6);

h) mettere a disposizione le **risorse** necessarie al funzionamento del SGSI;

i) promuovere la **consapevolezza** e la **formazione** del personale sulla sicurezza delle informazioni;

j) gestire gli **incidenti** di sicurezza e trarne insegnamento per migliorare;

k) **monitorare** il SGSI con audit interni condotti in modo obiettivo e imparziale e con il riesame della direzione, verificando nella formazione e negli audit interni che la politica sia compresa.

5. Principi

- **Riservatezza**: le informazioni sono accessibili solo a chi è autorizzato.
- **Integrità**: le informazioni sono accurate e complete, e protette da modifiche non autorizzate.
- **Disponibilità**: le informazioni e i servizi sono disponibili quando servono.
- **Minimizzazione**: si trattano solo i dati necessari alle finalità.
- **Privilegio minimo**: gli accessi si assegnano per gruppi, secondo il bisogno di conoscere per il proprio lavoro.

- **Classificazione**: ogni informazione ha una classe stabilita dal suo contenuto e si conserva in una sede di classe adeguata, secondo la *Politica di Classificazione delle Informazioni* (ID_520_PO_1).
- **Credenziali**: password, chiavi e segreti si custodiscono solo nel password manager, mai nei documenti.
- **Stessi standard per noi e per i clienti**: sui sistemi interni si applicano gli stessi standard di sicurezza e gli stessi strumenti professionali impiegati per i clienti.
- **Trasparenza sui limiti**: le carenze note si documentano e si trattano, con un'azione o con una decisione motivata; non si tacciono. Alle parti interessate si dichiarano soltanto le misure effettivamente applicate.

6. Obiettivi

Gli obiettivi di sicurezza delle informazioni di Techsystem sono:
a) proteggere i dati dei clienti che Techsystem tratta come responsabile del trattamento (ID_1136);
b) garantire la ripristinabilità dei dati e dei servizi, con backup verificati da prove di ripristino (ID_620_PO_1);
c) mantenere i sistemi aggiornati e protetti, gestendo gli aggiornamenti e le vulnerabilità tecniche (ID_1108);
d) custodire le credenziali in strumenti dedicati, fuori dai documenti condivisi;
e) governare i fornitori e i sub-responsabili del trattamento;
f) proteggere gli accessi e i dispositivi: identità centralizzata, con l'accesso alle postazioni e ai servizi aziendali tramite l'account Microsoft Entra ID; secondo fattore di autenticazione sull'account aziendale, sull'accesso remoto e sui pannelli di amministrazione; cifratura delle postazioni;
g) integrare la sicurezza nello sviluppo delle applicazioni interne (ID_1109) e governare l'uso degli strumenti di intelligenza artificiale (ID_1150).
Per ciascun obiettivo il Titolare stabilisce uno o più **indicatori misurabili** con il valore atteso, li documenta e ne riesamina il raggiungimento almeno **una volta l'anno**, nel riesame della direzione.

7. Servizi cloud

Techsystem **utilizza** servizi cloud di terzi ed **eroga** servizi cloud ai propri clienti.
a) **Come cliente di servizi cloud**, Techsystem sceglie i fornitori valutandone le garanzie di sicurezza e di protezione dei dati, e censisce i sub-responsabili del trattamento e l'ubicazione dei dati.
b) **Come fornitore di servizi cloud**, Techsystem:

- definisce e comunica ai clienti la ripartizione delle responsabilità di sicurezza fra Techsystem, il cliente e i fornitori dell'infrastruttura cloud;
- mantiene separati gli ambienti e i dati di ciascun cliente: ogni server in cloud è in una rete virtuale distinta, protetta dal proprio firewall; sui server di hosting condivisi ogni cliente ha utenze e database propri;
- amministra i server in cloud dal pannello del fornitore, con secondo fattore di autenticazione, oppure in SSH, raggiungibile solo dall'indirizzo IP della sede, e registra gli interventi nel registro del server o nel ticket del cliente;
- fornisce ai clienti informazioni adeguate per monitorare i servizi utilizzati;
- applica alle reti virtuali presso il fornitore gli stessi criteri della rete di sede: ogni rete è protetta da un firewall perimetrale che lascia aperte solo le porte necessarie al servizio.

c) **Per i dati personali trattati per conto dei clienti**, Techsystem:

- li tratta soltanto per erogare i servizi sottoscritti, secondo le istruzioni del cliente e il DPA (ID_1136), mai per finalità proprie, di marketing o di pubblicità;
- non accede al contenuto di posta, file e documenti dei clienti se non su loro richiesta;
- supporta il cliente nel riscontro alle richieste di esercizio dei diritti degli interessati;
- rende noti ai clienti i sub-responsabili e i Paesi in cui i dati possono essere trattati, e comunica in anticipo, con il preavviso previsto dal DPA, ogni aggiunta o sostituzione di sub-responsabili;
- informa il cliente delle richieste vincolanti di divulgazione dei dati da parte delle autorità, salvo che la legge lo vieti, e registra le divulgazioni effettuate;
- informa i clienti senza ingiustificato ritardo delle violazioni dei dati personali trattati per loro conto;
- vincola alla riservatezza il personale e i collaboratori che accedono ai dati, anche dopo la cessazione del rapporto;
- protegge con la cifratura i dati trasmessi su reti pubbliche e i supporti che escono dai locali aziendali, e assegna identificativi utente univoci a chi accede ai dati;
- al termine del servizio, a scelta del cliente, cancella o restituisce i dati, salvo gli obblighi di conservazione di legge.

8. Ruoli e responsabilità

- **Titolare** (Direzione): approva la presente politica e i documenti del SGSI; come Rappresentante della Direzione per il SGSI assicura che il SGSI sia conforme ai requisiti della norma e ne riferisce le prestazioni nel riesame della direzione; è responsabile della gestione del rischio, degli obiettivi e del riesame; assegna le risorse.
- **Responsabile Tecnico**: attua e verifica i controlli tecnici sull'infrastruttura interna e sui servizi erogati ai clienti; approva le registrazioni per le quali le procedure richiedono una seconda persona.
- **Personale tecnico**: applica le procedure tecniche ed esegue le verifiche ricorrenti assegnate.
- **Amministrazione**: tratta le informazioni amministrative e del personale secondo la ID_520_PO_1.
- **Tutto il personale**: rispetta la presente politica e le procedure che la attuano, prende visione dei documenti che gli sono destinati, **segnala subito al Titolare** gli eventi e gli incidenti di sicurezza, anche solo sospetti.

In ragione della dimensione dell'organizzazione, i ruoli sono attribuiti in forma **cumulata** e **proporzionata**; le responsabilità di dettaglio sono assegnate dalle singole procedure.

9. Politiche per tema e procedure

La presente politica è attuata dalle politiche per tema, dalle procedure e dalle istruzioni operative del SGSI **in vigore**, cioè quelle pubblicate dal Titolare sul modulo *Presa visione*, dove il personale le consulta. L'elenco aggiornato dei documenti del SGSI, con versione e stato di ciascuno, è il catalogo dei documenti nel *Portale applicazioni · modulo Stato SGSI*.

10. Comunicazione, adozione e riesame

La politica entra in vigore con la **pubblicazione** sul modulo *Presa visione* da parte del Titolare, ed è distribuita a tutto il personale con evidenza di presa visione.

È un documento **pubblico** (classe C0, ID_520_PO_1): è pubblicata sul sito web aziendale e si consegna senza restrizioni alle **parti interessate** che la richiedono — clienti, fornitori, ente di certificazione.
È riesaminata **annualmente** dalla data di adozione e comunque al verificarsi di cambiamenti significativi: organizzativi, tecnologici, normativi, contrattuali o dei servizi erogati.
Le **deroghe** alla presente politica e alle procedure che la attuano sono autorizzate dal Titolare, motivate, registrate con una scadenza e riesaminate alla scadenza.
Il mancato rispetto della presente politica e delle procedure che la attuano è valutato dal Titolare. Per il personale dipendente può dar luogo a provvedimenti disciplinari secondo il contratto collettivo applicato e l'art. 7 della L. 300/1970, con il supporto del consulente del lavoro; per collaboratori e fornitori, alle misure previste dai contratti.

Storico delle versioni

Versione	Data	Modifiche
0.1	13/07/2026	Prima bozza, mai adottata; inviata alla consulente il 23/07/2026 come allegato 02e.
0.2	18/10/2026	Bozza per l'adozione: codice D03 e *Controllo del documento*; edizioni delle norme; impegno sulla protezione dei dati personali trattati per conto dei clienti e sezione sui servizi cloud (§7); obiettivi con il quadro per renderli misurabili (§6); principio di classificazione allineato alla D04 v1.0; principio di trasparenza sui limiti; ruoli allineati («Titolare», «personale tecnico», Amministrazione); politiche per tema e procedure indicate come i documenti in vigore pubblicati sul modulo *Presa visione*, con rimando al catalogo del modulo *Stato SGSI* (§9); adozione e distribuzione tramite il modulo *Presa visione*; documento pubblico (C0); autorizzazione delle deroghe (§10).
1.0	21/10/2026	Prima versione in vigore. Integra gli spunti della Politica predisposta dalla consulente (ID_520): impegni della Direzione sulle clausole 5.1 e 5.3, valutazione dei rischi, audit interni e riesame (§4, §8); principio degli stessi standard per i sistemi interni e dichiarazione delle sole misure applicate (§5); obiettivi f) e g) (§6); impegni sui servizi cloud (27017) e sui dati personali dei clienti (27018) (§7). Campo di applicazione allineato alla D15 e rimando al Contesto (D20) (§2); pubblicazione sul sito web; trattamento del mancato rispetto (§10).
1.1	23/10/2026	Ricodifica (atto «Codifica dei documenti del Sistema di Gestione» (ID_1158) del 23/10/2026): codice ID_520 al posto di D03, rimandi con i codici nuovi; copertina e piè di pagina identificativo. Contenuto invariato.