

POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Impegno e obiettivi del sistema di gestione
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

Tekna S.r.l. adotta la presente Politica del Sistema di Gestione quale espressione formale della propria visione e dei propri impegni nei confronti della qualità dei servizi erogati, della protezione dell'ambiente, della salute e sicurezza sul lavoro e della sicurezza delle informazioni. Il documento traduce la missione aziendale in un quadro di riferimento unitario che orienta le decisioni strategiche e operative, promuovendo un equilibrio tra sviluppo economico, rispetto dell'ambiente, tutela delle persone e protezione del patrimonio informativo.

L'organizzazione riconosce che la sostenibilità del proprio modello di business nel settore dell'ingegneria civile e delle infrastrutture per telecomunicazioni dipende dalla capacità di integrare questi impegni nelle attività quotidiane di progettazione, direzione lavori, coordinamento per la sicurezza e collaudo, nonché nella consulenza tecnica ambientale. La presente politica fornisce pertanto il riferimento su cui si fondano gli obiettivi misurabili del Sistema di Gestione Integrato e le azioni per il loro conseguimento, in coerenza con gli indirizzi strategici e il contesto competitivo in cui Tekna opera.

Campo di applicazione

La presente politica si applica a tutte le attività e ai processi svolti da Tekna S.r.l. presso la sede operativa di Via Armando Diaz 41, 91025 Marsala (TP), relativi all'erogazione di servizi di progettazione, direzione dei lavori, coordinamento per la sicurezza e collaudo nel settore dell'ingegneria civile e impiantistica, nonché alla consulenza tecnica ambientale in materia di misurazioni di campo elettromagnetico e misure fonometriche, e alla verifica della progettazione delle opere ai fini della validazione. Coinvolge tutto il personale — dipendenti, collaboratori coordinati e terze parti con accesso ai sistemi e alle informazioni aziendali — e si estende ai rapporti con committenti, fornitori, partner commerciali, enti di controllo e altre parti interessate rilevanti.

Riferimenti normativi

- ISO 9001
- ISO 14001
- ISO 45001
- ISO/IEC 27001:2022
- D.Lgs. 81/2008
- Regolamento (UE) 2016/679

Termini e definizioni

- **Alta Direzione** : persona o gruppo di persone che, al livello più elevato, dirigono e controllano un'organizzazione, con l'autorità di delegare e rendere disponibili le risorse

necessarie.

- **Sistema di gestione** : insieme di elementi correlati o interagenti di un'organizzazione finalizzati a stabilire politiche, obiettivi e processi per conseguire tali obiettivi.
- **Politica** : intenzioni e indirizzo di un'organizzazione espressi formalmente dalla sua Alta Direzione.
- **Parte interessata** : persona od organizzazione che può influenzare, essere influenzata da, o percepirsi come influenzata da una decisione o attività.
- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere le prestazioni.
- **Informazione documentata** : informazione che è richiesto sia controllata e mantenuta dall'organizzazione, compreso il supporto su cui essa è contenuta.

Ruoli e responsabilità

- **Alta Direzione** : stabilisce, attua e mantiene aggiornata la politica aziendale, garantendo la sua coerenza con il contesto, gli indirizzi strategici e le esigenze delle parti interessate.
- **Responsabile del sistema di gestione** : supporta l'Alta Direzione nella formalizzazione della politica, ne cura la comunicazione interna ed esterna e ne propone l'aggiornamento in sede di riesame.

Impegno e obiettivi del sistema di gestione

L'Alta Direzione di Tekna S.r.l. esprime i seguenti impegni e principi, che costituiscono il quadro di riferimento per la definizione degli obiettivi del Sistema di Gestione Integrato e per l'orientamento delle decisioni a ogni livello dell'organizzazione.

Qualità dei servizi

Tekna persegue l'eccellenza nell'erogazione dei propri servizi di ingegneria civile e infrastrutture per telecomunicazioni, ponendo al centro la soddisfazione dei committenti e il rispetto dei requisiti contrattuali. L'organizzazione si impegna a comprendere e soddisfare le esigenze e le aspettative dei propri clienti — tra cui i principali operatori del settore telecomunicazioni — e a migliorare con continuità l'efficacia dei processi di progettazione, direzione lavori, coordinamento per la sicurezza e collaudo.

La politica per la qualità funge da quadro di riferimento per la definizione di obiettivi misurabili, riesaminati almeno annualmente nel corso del riesame della direzione, e si fonda sull'impegno a soddisfare i requisiti applicabili — di natura legislativa, regolamentare e contrattuale — nonché sul perseguimento del miglioramento continuo del sistema di gestione per la qualità.

Protezione dell'ambiente

Tekna riconosce la propria responsabilità nei confronti dell'ambiente in cui opera e si impegna alla protezione ambientale, inclusa la prevenzione dell'inquinamento, in modo appropriato alla natura, alla dimensione e agli impatti delle proprie attività.

L'organizzazione adotta un approccio proattivo volto a ridurre gli impatti ambientali associati ai servizi erogati, promuovendo l'uso responsabile delle risorse e la sensibilizzazione del personale verso pratiche sostenibili.

Tale impegno comprende il soddisfacimento degli obblighi di conformità legislativi e regolamentari applicabili, il miglioramento continuo delle prestazioni ambientali e la definizione di obiettivi ambientali coerenti con il contesto territoriale e le attività svolte presso la sede di Marsala e i siti dei committenti.

Salute e sicurezza sul lavoro

L'organizzazione è impegnata a garantire condizioni di lavoro sicure e salubri per la prevenzione di lesioni e malattie correlate al lavoro, adottando misure proporzionate ai rischi specifici delle proprie attività — in particolare le attività di ufficio tecnico e i sopralluoghi presso cantieri e siti tecnologici di terzi. L'impegno si estende all'eliminazione dei pericoli e alla riduzione dei rischi per la salute e sicurezza sul lavoro, attraverso un processo sistematico di identificazione, valutazione e trattamento condotto con il coinvolgimento attivo del personale.

Tekna promuove la consultazione e la partecipazione dei lavoratori e dei loro rappresentanti nelle decisioni che riguardano la salute e la sicurezza, riconoscendo il valore del contributo diretto di chi opera quotidianamente nei processi aziendali.

L'organizzazione si impegna altresì a soddisfare i requisiti legali e gli altri requisiti applicabili in materia di SSL e a perseguire il miglioramento continuo del sistema di gestione per la salute e sicurezza sul lavoro, definendo obiettivi che riflettano l'evoluzione del contesto normativo e operativo.

Sicurezza delle informazioni

Tekna riconosce il valore strategico del proprio patrimonio informativo e si impegna a proteggerne la riservatezza, l'integrità e la disponibilità, adottando un approccio basato sul rischio che tiene conto delle minacce e delle vulnerabilità proprie del settore dell'ingegneria e delle telecomunicazioni. L'organizzazione persegue obiettivi di sicurezza delle informazioni allineati agli indirizzi strategici e al contesto tecnologico in cui opera, garantendo che ogni persona con accesso ai sistemi informativi aziendali sia consapevole delle proprie responsabilità nella salvaguardia degli asset informativi.

L'impegno include il soddisfacimento dei requisiti applicabili in materia di sicurezza delle informazioni — derivanti dalla normativa, dai contratti con i committenti e dalle esigenze delle parti interessate — e il miglioramento continuo del sistema di gestione della sicurezza delle informazioni.

Comunicazione e disponibilità della politica

La presente politica è mantenuta come informazione documentata ed è comunicata a tutto il personale attraverso i canali interni approvati — e-mail aziendale, piattaforma Microsoft

Teams, sessioni formative dedicate e riunioni di team — affinché sia compresa e applicata a ogni livello dell'organizzazione. L'efficacia della comunicazione è attestata dalla conservazione di evidenze quali ricevute di presa visione, log di trasmissione, verbali delle riunioni e registri di partecipazione.

Per le parti interessate esterne, la politica è resa disponibile mediante pubblicazione sul sito web aziendale, inserimento nei contratti di fornitura e trasmissione via PEC ove sia richiesto valore legale, nel rispetto di quanto disciplinato dalla *PRO Procedura gestione comunicazione*.

Archiviazione e aggiornamento

La presente politica è conservata come informazione documentata all'interno del sistema di gestione documentale dell'organizzazione, sotto la responsabilità del **Responsabile del sistema di gestione**. Il riesame avviene almeno annualmente in concomitanza con il riesame della direzione, oppure ogni qualvolta si verificano cambiamenti significativi del contesto organizzativo, normativo o tecnologico. Ogni revisione è identificata da un numero progressivo di versione, approvata dall'Alta Direzione e comunicata al personale attraverso i canali interni approvati.

Documenti di riferimento

- PRO Processi direzionali
- PRO Procedura gestione comunicazione
- PRO Gestione riesame della direzione
- PRO Obiettivi e pianificazione per il loro raggiungimento

POL Politica di conservazione e cancellazione delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Principi di conservazione delle informazioni
- Piano di conservazione delle informazioni
- Cancellazione sicura delle informazioni
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica stabilisce il quadro di riferimento attraverso cui Tekna S.r.l. governa il ciclo di vita delle informazioni, dalla loro creazione sino alla cancellazione definitiva. L'organizzazione persegue un equilibrio consapevole tra le esigenze operative di continuità del servizio e gli obblighi legali, fiscali e contrattuali che impongono la conservazione di determinate categorie di dati per periodi definiti.

Tekna riconosce nel principio di limitazione della conservazione un valore fondamentale della propria gestione dei dati personali: nessuna informazione che consenta l'identificazione degli interessati viene mantenuta oltre il tempo strettamente necessario al conseguimento delle finalità per cui è stata raccolta. Al contempo, l'organizzazione si impegna a garantire che ogni informazione, al termine del proprio ciclo di vita utile, sia eliminata in modo sicuro e irrecuperabile, prevenendo qualsiasi rischio di accesso non autorizzato, divulgazione indebita o ricostruzione dei dati cancellati.

Questa politica costituisce il riferimento per tutte le decisioni relative alla durata di conservazione, alle modalità di archiviazione e ai metodi di cancellazione sicura adottati dall'organizzazione, contribuendo alla protezione del patrimonio informativo aziendale e alla conformità con il Sistema di Gestione della Sicurezza delle Informazioni.

Campo di applicazione

La presente politica si applica a tutte le informazioni create, ricevute, trattate o archiviate da Tekna S.r.l., indipendentemente dal formato — digitale o cartaceo — e dal supporto su cui risiedono, inclusi server, dispositivi utente, archivi fisici e servizi cloud utilizzati dall'organizzazione. Il suo ambito si estende alla sede operativa di Via Armando Diaz 41, Marsala (TP), a tutto il personale dipendente e ai collaboratori a qualsiasi titolo, nonché alle terze parti che gestiscono informazioni per conto dell'azienda.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Conservazione:** processo di mantenimento delle informazioni per un periodo di tempo predefinito e giustificato, in formato attivo o archiviato, al fine di soddisfare finalità operative, legali o contrattuali.
- **Cancellazione sicura:** processo che rende le informazioni irrecuperabili, garantendo che non possano essere ricostruite, lette o estratte da alcun supporto, neppure

attraverso tecniche forensi.

- **Archiviazione:** processo di trasferimento delle informazioni non più in uso attivo verso un ambiente di conservazione a lungo termine, sicuro e con accesso controllato.
- **Sospensione legale:** istruzione formale emessa dalla Direzione per sospendere le normali attività di cancellazione relative a specifiche informazioni, a causa di un contenzioso in corso, un'indagine o un audit.

Ruoli e responsabilità

- **Top Management:** supervisiona l'attuazione della presente politica, assicura la disponibilità delle risorse necessarie e dispone la sospensione legale della cancellazione quando richiesto da contenziosi, indagini o audit.
- **Responsabile del sistema di gestione:** gestisce e aggiorna il registro di conservazione delle informazioni e degli asset, coordina il riesame annuale dei periodi di conservazione e verifica la corretta esecuzione delle attività di cancellazione sicura.
- **Dipendenti, collaboratori e terze parti:** rispettano i periodi di conservazione definiti dalla presente politica, non mantengono copie non autorizzate di informazioni aziendali e provvedono allo smaltimento sicuro dei dati di propria competenza secondo le modalità stabilite.

Principi di conservazione delle informazioni

Tekna S.r.l. adotta un approccio alla conservazione delle informazioni fondato sulla proporzionalità e sulla giustificazione esplicita di ogni periodo di mantenimento. I dati personali non vengono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati.

L'organizzazione riconosce che la conservazione risponde a finalità di diversa natura, tra cui:

- **Finalità operative:** continuità dei servizi di progettazione, direzione lavori e consulenza tecnica che Tekna eroga ai propri committenti nel settore delle telecomunicazioni e dell'ingegneria civile.
- **Finalità legali e fiscali:** adempimento degli obblighi previsti dalla normativa tributaria, previdenziale e giuslavoristica, nonché gestione di eventuali contenziosi.
- **Finalità contrattuali:** soddisfacimento dei requisiti definiti dai committenti e conservazione della documentazione di progetto per il periodo concordato.
- **Finalità di sicurezza:** conservazione dei log e delle registrazioni necessarie a supportare indagini su eventi di sicurezza delle informazioni.

I periodi di conservazione stabiliti dall'organizzazione vengono riesaminati almeno una volta all'anno dal **Responsabile del sistema di gestione**, in collaborazione con il **Top Management**, per garantirne la continua adeguatezza e conformità rispetto all'evoluzione del contesto normativo e operativo. Qualora un'autorità giudiziaria, un'indagine interna o un

audit rendano necessaria la sospensione della cancellazione di specifiche informazioni, il **Top Management** emette formalmente un'istruzione di sospensione legale che prevale sui periodi di conservazione ordinari fino alla sua revoca.

Piano di conservazione delle informazioni

Tekna S.r.l. classifica le proprie informazioni e i propri asset in categorie logiche, a ciascuna delle quali associa un periodo di conservazione specifico, il tipo di supporto e la motivazione che ne giustifica la durata. Questa mappatura è documentata nel *MOD Conservazione delle informazioni e degli asset*, che costituisce il riferimento operativo per l'applicazione della presente politica.

Il registro riporta per ogni voce: la tipologia di record (informazione o asset), il supporto di conservazione (digitale, fisico o entrambi), il periodo di conservazione e la motivazione sottostante. A titolo esemplificativo, i periodi di conservazione tengono conto dei termini di prescrizione legale applicabili, della vita utile degli asset fisici e della rilevanza strategica delle informazioni per l'organizzazione.

Per quanto riguarda i dati personali, i termini di cancellazione sono coerenti con quanto documentato nel *MOD Registro dei trattamenti del titolare*, il quale specifica per ciascuna tipologia di trattamento i tempi di conservazione in relazione alle finalità e alle basi giuridiche applicabili.

Il **Responsabile del sistema di gestione** cura l'aggiornamento periodico del registro, sottoponendolo al riesame della Direzione almeno una volta l'anno e ogni volta che intervengano variazioni significative nella struttura dei trattamenti, negli obblighi normativi o nelle esigenze operative dell'organizzazione.

Cancellazione sicura delle informazioni

Tekna S.r.l. si impegna affinché ogni informazione, al termine del periodo di conservazione stabilito, venga eliminata in modo da renderne impossibile il recupero, anche mediante tecniche forensi avanzate. La scelta del metodo di cancellazione tiene conto della sensibilità dell'informazione e della natura del supporto su cui essa risiede.

Per i **supporti digitali**, l'organizzazione adotta i seguenti metodi:

- **Sovrascrittura multipla:** applicata ai supporti magnetici, assicura che i dati originali non possano essere ricostruiti.
- **Cancellazione crittografica:** consiste nella distruzione irreversibile della chiave di cifratura, rendendo permanentemente illeggibili i dati cifrati residui; è il metodo privilegiato per supporti SSD e volumi crittografati.
- **Smagnetizzazione o distruzione fisica:** riservata ai supporti che non consentono una cancellazione logica verificabile, quali hard disk danneggiati o nastri magnetici non più funzionanti. Lo smaltimento definitivo dei dispositivi dismessi avviene tramite fornitori qualificati per la gestione dei rifiuti elettronici.

Lo spazio di archiviazione riutilizzabile viene sottoposto a un processo di cancellazione sicura prima di ogni riassegnazione ad altro uso o ad altro utente, affinché nessun dato

residuo sia accessibile al nuovo destinatario.

Per i **supporti cartacei**, i documenti contenenti informazioni classificate come "confidential" o "limited" vengono distrutti mediante distruggi-documenti prima dello smaltimento.

Ogni operazione di cancellazione viene registrata indicando la data, l'identificativo del supporto, la tecnica utilizzata, l'esito dell'operazione e il responsabile che l'ha eseguita. I file temporanei generati dai sistemi nel corso delle normali operazioni vengono identificati e rimossi in modo sicuro quando non sono più necessari alle finalità per cui erano stati creati.

L'organizzazione promuove la consapevolezza del personale circa l'importanza della cancellazione sicura e assicura che le modalità operative descritte siano applicate in modo coerente dalla sede operativa e dalle terze parti che trattano informazioni per suo conto, in conformità con quanto previsto dalla *PRO Procedura di configurazione, gestione e smaltimento degli asset* per le attività di dismissione degli asset informatici.

Archiviazione e aggiornamento

La presente politica è un documento controllato del Sistema di Gestione della Sicurezza delle Informazioni. Viene conservata in formato elettronico con accesso in sola lettura per il personale autorizzato. Il **Responsabile del sistema di gestione** ne cura il riesame con cadenza almeno annuale, o in occasione di cambiamenti significativi nel contesto normativo, organizzativo o tecnologico. Ogni revisione segue il processo di approvazione definito dal Sistema di Gestione, incrementa il numero di versione ed è registrata nella documentazione di sistema. Le versioni superate vengono ritirate dalla circolazione e trasferite nell'archivio storico.

Documenti di riferimento

- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- MOD Conservazione delle informazioni e degli asset
- MOD Registro dei trattamenti del titolare

POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Definizione dei ruoli e responsabilità
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica stabilisce il quadro di riferimento attraverso il quale Tekna S.r.l. definisce, assegna e comunica i ruoli, le responsabilità e le autorità in materia di sicurezza delle informazioni. L'organizzazione riconosce che la protezione degli asset informativi — dalla documentazione progettuale riservata dei committenti telecomunicazioni ai dati personali del personale — richiede un'attribuzione chiara e univoca dei compiti a ogni livello della struttura organizzativa.

Attraverso questa politica l'organizzazione intende perseguire tre finalità complementari: garantire che ogni funzione aziendale comprenda il proprio contributo alla tutela della riservatezza, dell'integrità e della disponibilità delle informazioni; assicurare che le responsabilità di sicurezza siano integrate nelle mansioni quotidiane del personale, in coerenza con l'organigramma e il mansionario approvati dall'Alta Direzione; e promuovere una cultura della responsabilità condivisa in cui la segnalazione tempestiva degli eventi di sicurezza costituisca un obbligo individuale riconosciuto da ciascun operatore.

Campo di applicazione

La politica si applica a tutto il personale di Tekna S.r.l. — dipendenti a tempo indeterminato, collaboratori con contratto di collaborazione coordinata e continuativa e collaboratori a partita IVA con impegno continuativo superiore al 50 % — operante presso la sede di Via Armando Diaz 41, 91025 Marsala (TP). Rientrano nel perimetro anche le funzioni esterne contrattualizzate che trattano informazioni aziendali o accedono ai sistemi informativi dell'organizzazione, quali il Medico Competente e i professionisti esterni qualificati. La politica copre tutti i sistemi informativi, le piattaforme digitali e le infrastrutture di rete gestiti dall'organizzazione, nonché le informazioni su supporto fisico custodite presso la sede.

Riferimenti normativi

- ISO/IEC 27001
- GDPR

Termini e definizioni

- **Alta Direzione** : persona o gruppo di persone che dirigono e controllano un'organizzazione al più alto livello.
- **Ruolo** : insieme di responsabilità e autorità assegnate a una persona all'interno dell'organizzazione.
- **Autorità** : diritto attribuito a una persona di dare disposizioni e di prendere decisioni nell'ambito delle proprie funzioni.
- **Competenza** : capacità di applicare conoscenze e abilità per ottenere i risultati attesi.

- **Informazione documentata** : informazione che deve essere controllata e mantenuta da un'organizzazione e il supporto sul quale è contenuta.
- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata da, o percepire se stessa come influenzata da una decisione o attività.

Ruoli e responsabilità

- **Alta Direzione (Amministratore Unico)** : approva la presente politica, autorizza gli accessi ai sistemi IT critici e assicura le risorse necessarie al funzionamento del SGSI.
- **Responsabile del sistema di gestione** : gestisce le policy di sicurezza delle informazioni, coordina gli audit di sicurezza e verifica la coerenza tra la mappatura dei ruoli e l'organigramma vigente.
- **Responsabile Amministrativa / HR** : cura il trattamento sicuro dei dati amministrativi e del personale, gestisce gli accessi ai sistemi contabili con autenticazione a due fattori e supporta la comunicazione della presente politica al personale.
- **Personale tecnico e operativo** : rispetta le politiche e le procedure di sicurezza delle informazioni nell'utilizzo di sistemi, dispositivi e documentazione riservata dei committenti.

Definizione dei ruoli e responsabilità

Principi di assegnazione

Tekna S.r.l. fonda l'attribuzione delle responsabilità in materia di sicurezza delle informazioni su due principi complementari. Il primo è il principio di responsabilità condivisa: ogni persona che opera per conto dell'organizzazione contribuisce attivamente alla protezione degli asset informativi, in proporzione al livello di accesso e al tipo di informazioni trattate. Il secondo è il principio di integrazione organizzativa: le responsabilità di sicurezza non costituiscono un incarico separato, bensì sono parte integrante delle mansioni ordinarie di ciascun ruolo, come formalizzato nel *MOD Mansionario* e rappresentato nel *MOD Organigramma*.

L'assegnazione tiene conto delle esigenze specifiche dell'organizzazione — una micro-impresa di ingegneria operante nel settore delle telecomunicazioni e delle infrastrutture civili — dove la tutela della documentazione progettuale, dei dati dei committenti e delle misurazioni tecniche (campi elettromagnetici, fonometria) riveste un'importanza centrale per la continuità del business e la fiducia dei clienti.

Mappatura delle responsabilità per la sicurezza delle informazioni

La tabella seguente associa a ciascun livello organizzativo le responsabilità in materia di sicurezza delle informazioni, in coerenza con quanto documentato nel *MOD Mansionario*.

Livello / Ruolo	Responsabilità in materia di sicurezza delle informazioni
Alta Direzione (Amministratore Unico)	Titolare del trattamento dati; approva le policy di sicurezza e ne garantisce l'adeguatezza rispetto al contesto aziendale; autorizza gli accessi ai sistemi IT critici; assicura risorse umane, finanziarie e tecnologiche per il SGSI; richiede a tutto il personale di applicare la sicurezza delle informazioni in conformità alla politica e alle procedure; promuove il riesame periodico del SGSI.
Responsabile del sistema di gestione (RSGSI)	Responsabile del Sistema di Gestione Sicurezza delle Informazioni: gestisce le policy IT e le procedure di sicurezza; coordina la gestione degli accessi logici; pianifica e conduce gli audit interni di sicurezza; monitora gli indicatori di prestazione del SGSI; cura la formazione e la sensibilizzazione del personale; supporta l'Alta Direzione nel riesame e nel miglioramento continuo del sistema.
Responsabile Amministrativa / HR	Gestisce gli accessi ai sistemi amministrativi (FattureInCloud) con autenticazione a due fattori; tratta i dati amministrativi e del personale nel rispetto delle policy di sicurezza; assicura il rispetto delle policy DLP e delle regole sulle password; supporta la comunicazione e la distribuzione delle politiche di sicurezza al personale; raccoglie le firme di presa visione.
Personale tecnico – Direzione Lavori, Permitting, CSP/CSE	Accede alla documentazione progettuale e ai dati dei committenti riservati nel rispetto del principio di necessità; utilizza in modo accettabile i sistemi e i dispositivi aziendali; rispetta le policy di sicurezza durante le attività sul campo e in ufficio.
Personale tecnico – Project Management	Accede alla documentazione progettuale riservata necessaria al coordinamento delle commesse; garantisce l'uso

	accettabile dei sistemi informativi; rispetta le politiche di sicurezza delle informazioni.
Personale tecnico – TLC e Impianti, Progettazione e Strutture	Accede alla documentazione tecnica riservata, ai dati as-built e alle informazioni dei committenti; utilizza in modo accettabile i dispositivi, il NAS aziendale e i sistemi; rispetta le procedure di sicurezza nella gestione dei dati in campo.
Medico Competente (funzione esterna)	Tratta i dati sanitari dei lavoratori (categorie particolari ai sensi del GDPR) con massima riservatezza; assicura la conservazione sicura delle cartelle sanitarie in conformità alla normativa vigente.

Impegno dell'Alta Direzione

L'Alta Direzione di Tekna S.r.l. riconosce nella sicurezza delle informazioni un fattore abilitante per la fiducia dei committenti — in particolare operatori di telecomunicazioni e committenti di gare pubbliche e private — e per la continuità operativa dell'organizzazione. In tale prospettiva, l'Alta Direzione si impegna a:

- approvare la presente politica e verificarne periodicamente l'adeguatezza rispetto all'evoluzione del contesto organizzativo e delle minacce;
- comunicare i ruoli e le responsabilità di sicurezza a tutto il personale e verificarne la comprensione, anche tramite sessioni di sensibilizzazione;
- richiedere che ogni membro del personale applichi la sicurezza delle informazioni in conformità con la politica, le politiche specifiche per argomento e le procedure operative del SGSI;
- assicurare che le risorse necessarie — umane, finanziarie e tecnologiche — siano rese disponibili per il mantenimento e il miglioramento del sistema;
- riesaminare la presente politica in sede di Riesame della Direzione e deliberare eventuali adeguamenti.

Obblighi di tutto il personale

Ogni persona che opera per conto di Tekna S.r.l. è tenuta a comprendere e rispettare le responsabilità di sicurezza assegnate al proprio ruolo. L'organizzazione promuove in particolare l'osservanza delle seguenti condotte:

- applicare la politica di sicurezza delle informazioni, le politiche specifiche per argomento e le procedure operative nel proprio ambito di attività;
- partecipare alle attività formative programmate in materia di sicurezza delle informazioni, che comprendono il riconoscimento delle minacce di phishing, le buone prassi di

cybersecurity, la gestione delle password e il trattamento dei dati personali;

- segnalare tempestivamente al **Responsabile del sistema di gestione** o al proprio superiore gerarchico qualsiasi evento anomalo, vulnerabilità sospetta o violazione delle politiche di sicurezza;
- utilizzare le risorse informative esclusivamente per finalità aziendali autorizzate, nel rispetto dei principi di clean desk e clean screen;
- sottoscrivere la presa visione delle politiche di sicurezza all'atto dell'assunzione o dell'avvio della collaborazione e in occasione di ogni aggiornamento significativo.

Collegamento con la struttura organizzativa

La presente politica si integra con il quadro documentale dell'organizzazione secondo la logica seguente: il *MOD Organigramma* rappresenta graficamente le linee gerarchiche e funzionali approvate dall'Alta Direzione; il *MOD Mansionario* dettaglia per ciascuna posizione le responsabilità specifiche per framework ISO, comprese quelle relative alla sicurezza delle informazioni; la *PRO Procedura dei ruoli e responsabilità* disciplina le modalità operative di identificazione, assegnazione, comunicazione e riesame dei ruoli. L'aggiornamento della mappatura contenuta nella presente politica avviene in concomitanza con il riesame periodico dell'organigramma e del mansionario, oppure a seguito di cambiamenti significativi nell'assetto organizzativo, garantendo così la costante coerenza tra i documenti.

Archiviazione e aggiornamento

La presente politica è conservata in formato digitale sulla piattaforma documentale del Sistema di Gestione ed è accessibile a tutto il personale con classificazione "limitato". Il **Responsabile del sistema di gestione** ne cura la revisione almeno annuale, in concomitanza con il Riesame della Direzione, oppure a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia o nel contesto delle minacce. Ogni revisione richiede l'approvazione formale dell' **Alta Direzione** ; le versioni superate sono archiviate con indicazione della data di sostituzione e conservate per un periodo minimo di tre anni secondo le modalità stabilite nella *PRO Procedura di gestione delle informazioni documentate* .

Documenti di riferimento

- MOD Organigramma
- MOD Mansionario
- PRO Procedura dei ruoli e responsabilità
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione delle risorse umane
- POL Politica di sicurezza delle informazioni

POL Politica Gestione Conflitto d'interesse

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Principi fondamentali
- Esempi comuni di conflitto di interesse
- Fasi di gestione
- Conseguenze della Violazione
- Archiviazione e aggiornamento
- Documenti di Riferimento

Scopo

La presente Politica intende prevenire che i conflitti di interesse — reali, potenziali o percepiti — compromettano l'oggettività delle decisioni aziendali o dissimolino condotte riconducibili a fenomeni corruttivi. Tekna S.r.l. riconosce che la trasparenza nella gestione degli interessi personali costituisce un presidio essenziale per la tutela della propria reputazione, della fiducia dei clienti e dell'integrità del Sistema di Gestione Anticorruzione.

Attraverso questo documento l'organizzazione stabilisce i criteri per identificare, dichiarare, valutare e gestire le situazioni in cui interessi privati possono interferire — o anche solo apparire interferire — con gli interessi di Tekna S.r.l., assicurando che ogni decisione sia assunta sulla base di criteri esclusivamente oggettivi e meritocratici.

Campo di applicazione

La presente politica si applica all'Amministratore Unico, a tutti i dipendenti a tempo indeterminato e determinato, ai collaboratori coordinati e continuativi, ai consulenti e a chiunque agisca in nome o per conto di Tekna S.r.l. (collettivamente "i Destinatari"), presso la sede operativa di Via Armando Diaz 41, 91025 Marsala (TP). Rientrano nel perimetro di applicazione le attività di progettazione, direzione dei lavori, coordinamento per la sicurezza, collaudo, consulenza tecnica ambientale e verifica della progettazione erogate dall'organizzazione, con particolare attenzione ai processi commerciali e di partecipazione a gare d'appalto pubbliche e private nel settore delle telecomunicazioni e dell'ingegneria civile.

Riferimenti normativi

- ISO 37001:2016
- D.Lgs. 231/2001
- L. 190/2012
- D.P.R. 445/2000
- Art. 2391 Codice Civile

Termini e definizioni

- **Conflitto di interessi:** situazione in cui l'interesse privato di un Destinatario interferisce, o anche solo appare interferire, con gli interessi di Tekna S.r.l. L'interesse privato può consistere in un vantaggio finanziario o non finanziario per il Destinatario, per i suoi familiari, per persone a lui vicine o per entità con cui intrattiene un legame significativo.
- **Conflitto reale (o attuale):** l'interesse privato del Destinatario influenza già, o potrebbe concretamente influenzare, la sua obiettività in una decisione aziendale.

- **Conflitto potenziale:** l'interesse privato del Destinatario non è ancora in conflitto con quelli dell'organizzazione, ma la sua situazione personale o professionale potrebbe ragionevolmente condurre a un conflitto reale in futuro.
- **Conflitto apparente (o percepito):** un osservatore esterno ragionevole potrebbe percepire che l'interesse privato del Destinatario sia in grado di influenzare il suo giudizio, anche qualora ciò non stia effettivamente accadendo. Tale fattispecie risulta ugualmente lesiva perché erode la fiducia degli stakeholder e danneggia la reputazione dell'organizzazione.
- **Corruzione:** offerta, promessa, concessione, accettazione o sollecitazione di un indebito vantaggio di qualsiasi valore, in violazione della legge applicabile, come incentivo o ricompensa affinché una persona agisca o si astenga dall'agire in relazione all'esercizio delle proprie funzioni.
- **Funzione di conformità anticorruzione:** funzione cui è affidata la responsabilità di supervisionare la progettazione e l'attuazione del sistema di gestione per la prevenzione della corruzione.

Ruoli e responsabilità

- **Responsabile del sistema di gestione:** gestisce il Registro dei Conflitti di Interesse, coordina la raccolta periodica delle dichiarazioni, valuta la gravità dei conflitti segnalati e definisce le misure di mitigazione appropriate.
- L'Alta Direzione promuove una cultura in cui dichiarare un conflitto è riconosciuto come atto di trasparenza e lealtà, approva le misure di mitigazione più rilevanti e sottoscrive per prima la propria dichiarazione di assenza di conflitti di interesse.
- Ogni Destinatario riconosce autonomamente le situazioni di potenziale conflitto, le dichiara immediatamente compilando il *MOD Dichiarazione assenza conflitti di interesse*, si astiene da qualsiasi decisione correlata e aggiorna la propria dichiarazione al mutare delle circostanze.

Principi fondamentali

Tekna S.r.l. fonda la gestione dei conflitti di interesse su principi che orientano il comportamento di ciascun Destinatario e garantiscono la coerenza con il Sistema di Gestione Anticorruzione.

Priorità all'interesse aziendale. L'interesse dell'organizzazione prevale in ogni circostanza su qualsiasi interesse privato. Nessuna relazione personale, finanziaria o professionale esterna può giustificare una decisione contraria al bene dell'organizzazione o dei suoi clienti.

Dovere di trasparenza. Il dovere primario di ogni Destinatario consiste nel dichiarare qualsiasi conflitto — reale, potenziale o apparente — non appena ne venga a conoscenza. La dichiarazione non costituisce un'ammissione di colpa: è la mancata dichiarazione a rappresentare una violazione della presente politica e del rapporto di fiducia con l'organizzazione. Nel dubbio, la regola è dichiarare.

Astensione immediata. In attesa che il conflitto dichiarato sia valutato e gestito, il Destinatario si astiene da qualsiasi discussione, deliberazione o attività decisionale relativa alla materia in conflitto, garantendo così l'imparzialità del processo.

Imparzialità decisionale. Le decisioni aziendali — in particolare quelle relative alla selezione dei fornitori, alla partecipazione a gare d'appalto, alle assunzioni e alle promozioni — si fondano esclusivamente su criteri oggettivi, meritocratici e documentabili, in coerenza con quanto previsto dal *Codice di condotta* e dalla *POL Politica del Sistema di Gestione Anticorruzione*.

Esempi comuni di conflitto di interesse

L'elenco che segue, senza pretesa di esaustività, illustra le situazioni più ricorrenti nel contesto operativo di Tekna S.r.l., al fine di agevolare l'autovalutazione da parte dei Destinatari.

Interessi finanziari. Detenere una quota di proprietà o interessi finanziari significativi in un fornitore, cliente, concorrente o partner di raggruppamento temporaneo di imprese con cui Tekna S.r.l. intrattiene rapporti commerciali — ad eccezione di partecipazioni minime in società quotate pubblicamente — configura un potenziale conflitto ogniqualvolta il Destinatario partecipi a decisioni che coinvolgono tali soggetti.

Relazioni familiari e personali. Partecipare al processo di selezione, valutazione, promozione o determinazione del compenso di un familiare o di una persona con cui si intrattiene una relazione sentimentale rappresenta un conflitto rilevante. Analogamente, gestire la relazione con un fornitore o un cliente presso il quale un familiare o un partner detenga una posizione di rilievo genera una situazione che richiede immediata dichiarazione.

Doppi incarichi e attività esterne. Svolgere un secondo incarico — anche a titolo di consulenza — per un concorrente, un fornitore o un cliente di Tekna S.r.l., oppure accettare posizioni in consigli di amministrazione o comitati tecnici esterni senza preventiva comunicazione all'organizzazione, costituisce un conflitto potenziale da valutare.

Utilizzo di risorse o informazioni aziendali. Sfruttare informazioni riservate apprese nel corso dell'attività lavorativa per un tornaconto personale o per avviare un'attività concorrente, così come impiegare beni, attrezzature o know-how aziendale per finalità estranee al rapporto con Tekna S.r.l., configura un conflitto reale e una violazione degli obblighi di riservatezza contrattualmente assunti.

Regali e ospitalità. Accettare o offrire regali, ospitalità o favori che eccedano le soglie di modico valore definite nella *PRO Procedura gestione dei regali/ donazioni/ sponsorizzazioni* può generare un'apparenza di obbligo o condizionamento, integrando un conflitto apparente particolarmente rilevante nei rapporti con la Pubblica Amministrazione e con i committenti pubblici.

Fasi di gestione

Tekna S.r.l. adotta un approccio strutturato alla gestione dei conflitti di interesse, articolato in fasi che garantiscono trasparenza, tracciabilità e proporzionalità delle misure.

Fase 1: Identificazione e Dichiarazione

L'organizzazione promuove l'autovalutazione continua da parte di ogni Destinatario: non appena un soggetto ritenga di trovarsi in una situazione di conflitto — reale, potenziale o apparente — è tenuto ad interrompere qualsiasi coinvolgimento nel processo decisionale correlato, a compilare il *MOD Dichiarazione assenza conflitti di interesse* e a trasmetterlo al **Responsabile del sistema di gestione**. Il principio guida è che, nel dubbio, la dichiarazione è sempre preferibile all'omissione.

Indipendentemente dalle dichiarazioni ad hoc, Tekna S.r.l. richiede a tutto il personale — e in particolare ai soggetti che ricoprono funzioni in ambito commerciale, di gestione acquisti e di direzione lavori — la compilazione annuale di una dichiarazione di assenza (o presenza) di conflitti di interesse, secondo le modalità previste dalla *PRO Procedura di gestione delle risorse umane*. La prima dichiarazione è raccolta al momento dell'instaurazione del rapporto di lavoro o di collaborazione.

Fase 2: Valutazione e Mitigazione

Ricevuta la dichiarazione, il **Responsabile del sistema di gestione** ne analizza la natura, la gravità e il rischio per l'organizzazione, eventualmente approfondendo i fatti con il dichiarante. Sulla base della valutazione, l'organizzazione adotta la misura di mitigazione più appropriata tra le seguenti, ordinate dalla meno alla più incisiva:

- **Monitoraggio:** la situazione viene registrata e sorvegliata nel tempo, soluzione adeguata per i conflitti meramente apparenti o a basso rischio.
- **Astensione formale:** il Destinatario è escluso permanentemente dal processo decisionale specifico.
- **Riassegnazione:** il Destinatario viene ricollocato su altre attività o progetti privi di connessione con il conflitto.
- **Neutralizzazione:** l'organizzazione richiede al Destinatario di eliminare la fonte del conflitto (ad esempio cedere quote, interrompere un incarico esterno) oppure interrompe la relazione con la terza parte coinvolta.

Qualora il conflitto coinvolga direttamente l'Alta Direzione, la valutazione e la decisione sulle misure sono assunte con il supporto del **Responsabile del sistema di gestione** e, ove necessario, con il coinvolgimento di consulenti esterni indipendenti, al fine di garantire l'imparzialità del processo.

Fase 3: Registrazione

Tutte le dichiarazioni, le valutazioni effettuate e le misure di mitigazione adottate sono archiviate in modo riservato nel Registro dei Conflitti di Interesse, gestito dal **Responsabile del sistema di gestione**. Il registro assicura la piena tracciabilità ai fini di audit e di riesame da parte dell'Alta Direzione, in coerenza con i requisiti di ISO 37001. Le informazioni contenute nel registro sono classificate come riservate e accessibili unicamente ai soggetti autorizzati.

Conseguenze della Violazione

La mancata dichiarazione di un conflitto di interesse, la deliberata occultazione di una situazione rilevante o la violazione delle misure di mitigazione imposte configurano un'infrazione grave del rapporto di fiducia e una violazione del *Codice di condotta* e della *POL Politica del Sistema di Gestione Anticorruzione*.

Tekna S.r.l. persegue tali violazioni con determinazione, applicando le sanzioni previste dal CCNL Studi Professionali – Consilp e dalla disciplina civilistica in materia di obblighi di fedeltà e diligenza (artt. 2104 e 2105 del Codice Civile). Le conseguenze possono comprendere provvedimenti disciplinari proporzionati alla gravità, fino alla risoluzione del rapporto di lavoro per giusta causa ai sensi dell'art. 2119 del Codice Civile, oltre alla richiesta di risarcimento dei danni patrimoniali e non patrimoniali eventualmente causati all'organizzazione.

Per i collaboratori esterni, i consulenti e i partner commerciali, la violazione della presente politica determina la facoltà dell'organizzazione di risolvere il rapporto contrattuale con effetto immediato e di escludere il soggetto da future collaborazioni, ferma restando ogni ulteriore azione legale a tutela dei propri interessi.

Archiviazione e aggiornamento

La presente politica è un documento controllato del Sistema di Gestione Anticorruzione. Il **Responsabile del sistema di gestione** ne cura la conservazione in formato digitale e ne assicura la disponibilità a tutti i Destinatari. La politica è sottoposta a riesame con cadenza almeno annuale — o in occasione di cambiamenti significativi nell'organizzazione, nel contesto normativo o nel profilo di rischio anticorruzione — e le eventuali modifiche sono approvate dall'Alta Direzione e comunicate tempestivamente al personale.

Documenti di Riferimento

- POL Politica del Sistema di Gestione Anticorruzione
- Codice di condotta
- PRO Procedura gestione dei regali/ donazioni/ sponsorizzazioni
- PRO Procedura di gestione delle segnalazioni
- PRO Procedura di due diligence
- PRO Procedura di gestione delle risorse umane
- MOD Dichiarazione assenza conflitti di interesse
- MOD valutazione e approvazione offerte

POL Politica anticorruzione per i partner commerciali

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Comportamenti e condotte accettabili
- Comportamenti e condotte inaccettabili
- Segnalazione di violazioni
- Conseguenze disciplinari
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente Politica definisce i requisiti anticorruzione che Tekna S.r.l. rivolge ai propri partner commerciali — fornitori, consulenti, collaboratori esterni e partner di raggruppamenti temporanei di impresa — affinché l'intera catena del valore aderisca agli standard di integrità e prevenzione della corruzione adottati dall'organizzazione. Tekna promuove una cultura d'impresa fondata sulla trasparenza e sulla legalità, riconoscendo che la credibilità dei propri servizi di ingegneria e delle infrastrutture di telecomunicazione dipende anche dalla condotta etica di chi opera per suo conto o a suo vantaggio.

Attraverso questo documento, l'organizzazione comunica le aspettative di conformità, i comportamenti accettabili e le condotte vietate, i meccanismi di segnalazione e le conseguenze disciplinari applicabili a tutti i soggetti che intrattengono rapporti commerciali con Tekna S.r.l.

Campo di applicazione

La presente Politica si applica a tutti i rapporti tra Tekna S.r.l. e i propri partner commerciali, indipendentemente dalla sede operativa, dalla durata o dal valore economico della collaborazione. In particolare, essa copre:

- fornitori di servizi professionali in outsourcing (direzione lavori, coordinamento sicurezza, progettazione infrastrutture TLC);
- partner di insourcing integrati nei processi operativi (raggruppamenti temporanei di impresa, partner progettuali);
- consulenti tecnici, legali, fiscali e amministrativi;
- fornitori di beni e servizi generali;
- qualsiasi terza parte che interagisca con pubblici ufficiali o enti della pubblica amministrazione per conto di Tekna S.r.l.

Restano esclusi dall'ambito della presente Politica i rapporti con società controllate o collegate, in quanto Tekna S.r.l. è una società indipendente priva di partecipazioni societarie.

Riferimenti normativi

- ISO 37001
- L. 190/2012
- D.Lgs. 231/2001
- D.Lgs. 24/2023

Termini e definizioni

- **Corruzione** : offrire, promettere, dare, accettare o richiedere un vantaggio indebito di qualsiasi natura, direttamente o attraverso intermediari, allo scopo di indurre o ricompensare una persona affinché compia o ometta un atto in violazione dei propri doveri.
- **Sistema di gestione per la prevenzione della corruzione** : insieme di elementi correlati o interagenti di un'organizzazione finalizzati a stabilire politiche e obiettivi anticorruzione e a conseguirli.
- **Funzione di conformità per la prevenzione della corruzione** : persona o unità organizzativa alla quale è attribuita la responsabilità e l'autorità per il funzionamento del sistema di gestione per la prevenzione della corruzione.
- **Pagamenti di facilitazione** : pagamenti non ufficiali di piccola entità effettuati per accelerare o assicurare l'esecuzione di un'azione di routine o necessaria alla quale il pagante ha già diritto.
- **Socio in affari** : parte esterna con la quale l'organizzazione intrattiene, o prevede di instaurare, una qualche forma di rapporto commerciale.
- **Due diligence** : processo di valutazione della natura e dell'entità dei rischi di corruzione e finalizzato ad assistere l'organizzazione nel prevenire, identificare e affrontare la corruzione.

Ruoli e responsabilità

- **Top Management** : approva la presente Politica, ne garantisce la comunicazione ai partner commerciali e supervisiona l'adeguatezza delle misure anticorruzione adottate nella catena del valore.
- **Responsabile del sistema di gestione** : verifica l'accettazione della Politica da parte dei partner in fase di qualifica, monitora la conformità anticorruzione durante il rapporto commerciale, gestisce le segnalazioni e propone azioni correttive.
- **Partner commerciali** : leggono, comprendono e aderiscono integralmente ai principi e alle regole della presente Politica, segnalano tempestivamente qualsiasi sospetto di violazione e collaborano nelle attività di verifica condotte dall'organizzazione.

Comportamenti e condotte accettabili

Tekna S.r.l. si attende che ogni partner commerciale operi secondo i principi di seguito esposti, mantenendo un comportamento coerente con lo spirito anticorruzione dell'organizzazione.

Integrità e conformità legale

L'organizzazione si attende dai propri partner un impegno continuo a operare nel pieno rispetto di tutte le leggi e i regolamenti anticorruzione applicabili nei paesi in cui svolgono attività. Tekna adotta una posizione di tolleranza zero verso qualsiasi forma di corruzione, attiva o passiva, pubblica o privata, e richiede ai partner di condividere tale impegno rifiutando attivamente qualsiasi condotta illecita.

In materia di omaggi, pasti e forme di cortesia commerciale, l'organizzazione ritiene accettabile soltanto ciò che risulta di modico valore, occasionale, trasparente, debitamente registrato e mai finalizzato a influenzare impropriamente una decisione. I limiti e le modalità di approvazione sono definiti nella *PRO Procedura gestione dei regali/ donazioni/ sponsorizzazioni*. Donazioni e sponsorizzazioni sono ammesse esclusivamente quando effettuate in modo trasparente, legale e tracciabile, previa verifica che non rappresentino un mezzo per mascherare atti corruttivi.

Trasparenza e concorrenza

Tekna promuove la libera concorrenza e si attende che i propri partner competano lealmente sul mercato, senza stipulare accordi illeciti, spartizioni di mercati o intese in violazione delle norme antitrust. L'organizzazione valorizza la trasparenza e richiede la comunicazione proattiva di qualsiasi potenziale conflitto d'interesse — reale, potenziale o apparente — inclusi legami familiari, finanziari o professionali con personale di Tekna. Le modalità di dichiarazione e gestione dei conflitti d'interesse sono disciplinate nella *POL Politica Gestione Conflitto d'Interesse*.

I partner commerciali sono tenuti a mantenere registrazioni contabili, fatture e documenti commerciali accurati, completi e veritieri, che riflettano fedelmente tutte le transazioni intercorse con Tekna S.r.l.

Diritti umani e lavoro

L'organizzazione riconosce la dignità della persona come valore fondamentale e si attende che i partner rispettino i diritti umani fondamentali, vietando rigorosamente qualsiasi forma di lavoro forzato, obbligato o minorile. L'impegno si estende alla garanzia di un ambiente di lavoro sicuro e salubre, conforme alla normativa vigente, e alla non discriminazione nelle decisioni relative al personale.

Riservatezza e collaborazione

I partner commerciali che accedono a informazioni riservate di Tekna si impegnano a tutelarne la riservatezza, utilizzandole esclusivamente per gli scopi concordati e prevenendone la divulgazione non autorizzata, nel pieno rispetto della normativa sulla protezione dei dati personali. L'organizzazione attribuisce particolare importanza alla collaborazione attiva durante eventuali attività di verifica, due diligence o audit di conformità anticorruzione.

I partner sono inoltre incoraggiati a promuovere presso i propri dipendenti una cultura della segnalazione, affinché qualsiasi sospetto di violazione della presente Politica venga comunicato tempestivamente attraverso i canali disponibili.

Comportamenti e condotte inaccettabili

Tekna S.r.l. vieta categoricamente ai propri partner commerciali le seguenti condotte, la cui violazione costituisce grave inadempimento contrattuale:

- **Corruzione attiva e passiva** : qualsiasi atto corruttivo, diretto o per il tramite di intermediari, volto a influenzare l'operato di un pubblico ufficiale, di un funzionario privato o di qualsiasi altro soggetto.
- **Pagamenti di facilitazione** : esecuzione o autorizzazione di pagamenti non ufficiali finalizzati ad accelerare pratiche amministrative, indipendentemente dall'importo o dalla prassi locale. L'unica eccezione ammessa riguarda situazioni di comprovato pericolo per la vita, con obbligo di segnalazione immediata.
- **Occultamento di fondi** : creazione di fondi non registrati, conti occulti o registrazioni contabili false o fuorvianti.
- **Ritorsioni** : qualsiasi atto ritorsivo, discriminatorio o punitivo nei confronti di chi segnali in buona fede un sospetto di corruzione o partecipi a un'indagine.
- **Omissione della dichiarazione di conflitti d'interesse** : l'instaurazione o il mantenimento di rapporti commerciali senza aver dichiarato conflitti d'interesse reali, potenziali o apparenti.
- **Mancata cooperazione nelle verifiche** : il rifiuto di collaborare in buona fede durante le attività di due diligence o di audit anticorruzione condotte da Tekna S.r.l.

Segnalazione di violazioni

Tekna S.r.l. promuove una cultura della segnalazione quale strumento essenziale per la prevenzione e l'individuazione di condotte illecite. Chiunque — personale del partner commerciale, collaboratori o terze parti — sia testimone o venga a conoscenza di un comportamento che viola la presente Politica è tenuto a segnalarlo tempestivamente e in modo confidenziale.

Le segnalazioni possono essere effettuate attraverso:

- la piattaforma digitale crittografata di whistleblowing messa a disposizione dall'organizzazione, che consente il dialogo bidirezionale anche in forma anonima;
- comunicazione scritta riservata indirizzata al **Responsabile del sistema di gestione** presso la sede di Via Armando Diaz 41, 91025 Marsala (TP);
- il canale esterno presso l'Autorità Nazionale Anticorruzione (ANAC), accessibile qualora i canali interni risultino indisponibili, non conformi o in caso di fondato timore di ritorsione.

Tekna S.r.l. garantisce la massima riservatezza dell'identità del segnalante e vieta categoricamente qualsiasi forma di ritorsione nei confronti di chi segnali in buona fede una violazione o partecipi a un'indagine. L'identità del segnalante non può essere rivelata senza il suo consenso esplicito. Ogni atto ritorsivo accertato è considerato nullo e costituisce a sua volta una grave violazione disciplinare.

Le violazioni oggetto di segnalazione comprendono, in via esemplificativa:

- illeciti amministrativi, contabili, civili o penali;
- violazioni della normativa europea in materia di appalti pubblici, prevenzione del riciclaggio, tutela dell'ambiente, protezione dei dati personali e concorrenza;
- atti od omissioni che ledano gli interessi finanziari dell'Unione Europea;

- qualsiasi condotta riconducibile a fenomeni corruttivi ai sensi della presente Politica.

Conseguenze disciplinari

La violazione della presente Politica costituisce un grave inadempimento degli obblighi contrattuali e comporta l'adozione di misure proporzionate alla gravità della condotta. Il **Top Management**, sentito il **Responsabile del sistema di gestione**, valuta ogni caso e adotta le misure ritenute appropriate.

Per i rapporti con partner commerciali, le conseguenze possono includere:

- richiesta formale di azioni correttive con tempistiche definite;
- sospensione cautelativa del rapporto contrattuale in pendenza di accertamenti;
- risoluzione immediata del contratto per giusta causa;
- esclusione permanente dall'elenco dei fornitori qualificati;
- segnalazione alle autorità competenti, fatte salve le responsabilità penali individuali.

I casi accertati di corruzione — attiva o passiva — comportano la risoluzione immediata del rapporto contrattuale, senza necessità di preavviso e con riserva di ogni azione risarcitoria.

Archiviazione e aggiornamento

Il presente documento è gestito come informazione documentata controllata. Viene archiviato in formato digitale e sottoposto a revisione periodica, con cadenza almeno annuale, o a seguito di cambiamenti significativi che ne impattino l'applicabilità — quali modifiche normative, variazioni organizzative o esiti di audit. La gestione e l'aggiornamento sono di competenza del **Responsabile del sistema di gestione**.

Documenti di riferimento

- POL Politica del Sistema di Gestione Anticorruzione
- PRO Procedura di gestione delle segnalazioni
- PRO Procedura di due diligence
- PRO Procedura gestione dei regali/ donazioni/ sponsorizzazioni
- POL Politica Gestione Conflitto d'Interesse

POL Politica del Sistema di Gestione Anticorruzione

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi strategici di anticorruzione
- Principi operativi fondamentali e controlli chiave
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente Politica esprime la posizione formale di Tekna S.r.l. nei confronti della prevenzione e del contrasto alla corruzione in tutte le sue forme. Attraverso questo documento, l'Alta Direzione dichiara l'impegno dell'organizzazione a operare con integrità, trasparenza e piena conformità alle leggi anticorruzione applicabili, adottando una posizione di tolleranza zero verso qualsiasi condotta corruttiva, sia attiva sia passiva, nel settore pubblico come in quello privato.

La Politica costituisce il quadro di riferimento per la definizione degli obiettivi anticorruzione e per l'orientamento delle decisioni strategiche e operative dell'organizzazione. Essa incoraggia la segnalazione in buona fede di qualsiasi sospetto, in modo confidenziale e senza timore di ritorsioni, e riafferma l'impegno al miglioramento continuo del Sistema di Gestione Anticorruzione (SGAC). Ogni membro del personale, ogni collaboratore e ogni partner commerciale è chiamato a conoscere, comprendere e applicare i principi qui enunciati, contribuendo a una cultura aziendale fondata sull'etica e sulla legalità.

Campo di applicazione

La presente Politica si applica a Tekna S.r.l. presso la sede legale e operativa di Via Armando Diaz 41, 91025 Marsala (TP), con riferimento all'erogazione di servizi di progettazione, direzione dei lavori, coordinamento per la sicurezza e collaudo nel settore dell'ingegneria civile e impiantistica, alla consulenza tecnica ambientale e alla verifica della progettazione delle opere. Il suo rispetto è vincolante per l'Alta Direzione, tutto il personale dipendente, i collaboratori coordinati e il personale temporaneo che agisce sotto la direzione e il controllo dell'organizzazione. L'organizzazione estende le proprie aspettative di integrità ai partner commerciali — fornitori, consulenti, subappaltatori e qualsiasi soggetto che agisca per conto o nell'interesse di Tekna — esercitando una ragionevole influenza contrattuale affinché aderiscano a principi anticorruzione coerenti con quelli della presente Politica.

Riferimenti normativi

- ISO 37001
- D.Lgs. 231/2001
- D.Lgs. 24/2023
- Legge 190/2012

Termini e definizioni

- **Corruzione** : offrire, promettere, dare, accettare o sollecitare un vantaggio indebito di qualsiasi valore, direttamente o indirettamente, al fine di indurre o premiare una persona affinché agisca o si astenga dall'agire in relazione alla prestazione dei propri doveri.

- **Sistema di gestione anticorruzione** : insieme di elementi correlati o interagenti di un'organizzazione finalizzati a stabilire politiche e obiettivi in materia di prevenzione della corruzione, nonché i processi per conseguire tali obiettivi.
- **Funzione di conformità anticorruzione** : persona o struttura alla quale l'organizzazione affida la responsabilità e l'autorità di supervisionare la progettazione e l'attuazione del sistema di gestione anticorruzione.
- **Due diligence** : processo per approfondire la natura e l'entità dei rischi di corruzione e per aiutare l'organizzazione a prendere decisioni relative a specifiche transazioni, progetti, attività, partner commerciali e membri del personale.
- **Partner commerciale** : parte esterna con la quale l'organizzazione ha, o prevede di stabilire, una qualche forma di rapporto d'affari.

Ruoli e responsabilità

- **Alta Direzione** : approva e riesamina periodicamente la presente Politica e gli obiettivi anticorruzione, garantisce l'allocazione di risorse adeguate al SGAC e promuove a tutti i livelli una cultura di integrità e tolleranza zero verso la corruzione.
- **Responsabile del sistema di gestione** : opera quale funzione di conformità anticorruzione, supervisionando l'attuazione quotidiana del SGAC, fornendo consulenza interpretativa sulla Politica, monitorando i controlli anticorruzione e riferendo direttamente all'Alta Direzione sulle prestazioni del sistema.

Obiettivi strategici di anticorruzione

Tekna persegue obiettivi anticorruzione coerenti con il proprio contesto operativo nel settore dell'ingegneria civile e delle infrastrutture per telecomunicazioni, dove l'interazione con enti pubblici per permessi e autorizzazioni rappresenta un'area di particolare attenzione. Gli obiettivi sono riesaminati almeno annualmente nell'ambito del riesame della direzione e documentati nel programma di miglioramento.

L'organizzazione si impegna a mantenere la piena conformità alle leggi anticorruzione vigenti, assicurando che ogni processo aziendale — dalla fase commerciale alla gestione dei subappalti — integri i requisiti del SGAC. L'identificazione e la valutazione dei rischi di corruzione costituiscono un'attività ricorrente, finalizzata a calibrare i controlli interni sulle aree effettivamente più esposte, quali le relazioni con la Pubblica Amministrazione, l'approvvigionamento e la partecipazione a gare d'appalto.

La sensibilizzazione e la formazione del personale rappresentano un pilastro degli obiettivi anticorruzione: l'organizzazione garantisce che tutto il personale riceva formazione mirata almeno annualmente, con contenuti differenziati per ruolo e livello di esposizione al rischio. Anche i partner commerciali che presentano un rischio superiore al livello minimo ricevono le informazioni necessarie per aderire alle aspettative anticorruzione dell'organizzazione.

Il miglioramento continuo dell'efficacia del SGAC è perseguito attraverso il monitoraggio di indicatori chiave — quali gli esiti degli audit interni, le segnalazioni ricevute e lo stato di completamento della formazione — e attraverso l'attuazione tempestiva delle azioni correttive necessarie.

Principi operativi fondamentali e controlli chiave

Tekna fonda il proprio Sistema di Gestione Anticorruzione su un insieme di principi e controlli che permeano ogni ambito dell'attività aziendale, dalla progettazione ingegneristica alla gestione dei rapporti con committenti e fornitori.

Divieto assoluto di corruzione e pagamenti di facilitazione. L'organizzazione vieta rigorosamente qualsiasi atto, diretto o indiretto, riconducibile a corruzione — incluse tangenti, regalie eccessive, finanziamenti illeciti e qualsiasi scambio finalizzato a influenzare indebitamente una decisione. I pagamenti di facilitazione sono vietati in modo categorico, indipendentemente dall'importo o dalla prassi locale. Il personale che riceve una richiesta in tal senso è tenuto a rifiutarla e a segnalarla immediatamente al

Responsabile del sistema di gestione .

Regali, donazioni e sponsorizzazioni. L'accettazione o l'offerta di omaggi è disciplinata dalla *PRO Procedura gestione dei regali/ donazioni/ sponsorizzazioni* , che stabilisce soglie monetarie, livelli di approvazione differenziati in base al valore e al destinatario, e un divieto assoluto per i regali in denaro contante o equivalenti. Ogni donazione e sponsorizzazione richiede un'analisi di rischio e un'approvazione formale documentata; i rapporti con Pubblici Ufficiali sono soggetti a restrizioni rafforzate. Il registro dei regali è conservato per un periodo minimo di dieci anni.

Due diligence sui partner commerciali. Tekna si impegna ad esercitare una due diligence proporzionata al rischio di corruzione su fornitori, subappaltatori e consulenti, verificando l'assenza di precedenti negativi, la regolarità fiscale e la solidità etica prima di instaurare rapporti d'affari. I partner commerciali sono tenuti a sottoscrivere clausole anticorruzione nei relativi accordi contrattuali, la cui violazione può comportare la risoluzione immediata del rapporto.

Controlli finanziari e tracciabilità. L'organizzazione mantiene registri contabili completi e accurati che riflettono fedelmente tutte le transazioni. È vietata la creazione di fondi non registrati o la falsificazione di documenti contabili. Per le transazioni superiori a soglie predefinite è richiesta una doppia autorizzazione; tutte le richieste di acquisto e gli ordini di servizio devono essere emessi attraverso canali scritti con ambiti di lavoro e prezzi predefiniti.

Segnalazione e protezione dei segnalanti. Tekna incoraggia attivamente la segnalazione — anche anonima — di qualsiasi sospetto di corruzione o violazione della presente Politica. Sono predisposti canali sicuri, riservati e accessibili a tutto il personale e alle terze parti, conformi al D.Lgs. 24/2023: una piattaforma informatica dedicata che garantisce crittografia e dialogo anonimo bidirezionale, un canale scritto mediante busta chiusa indirizzata al Gestore delle Segnalazioni, e la possibilità di un incontro orale riservato. L'identità del segnalante non può essere rivelata senza il suo esplicito consenso. L'organizzazione vieta categoricamente qualsiasi forma di ritorsione — inclusi demansionamento, discriminazione, mobbing e licenziamento ingiustificato — nei confronti di chiunque segnali in buona fede o rifiuti di partecipare ad atti di corruzione, anche qualora tale rifiuto comporti la perdita di opportunità commerciali.

Conseguenze del mancato rispetto della Politica. La violazione della presente Politica, delle procedure correlate o delle leggi anticorruzione applicabili comporta conseguenze disciplinari proporzionate alla gravità dell'infrazione, fino alla risoluzione del rapporto di

lavoro per giusta causa e alla richiesta di risarcimento danni. Per i collaboratori esterni e i partner commerciali, la violazione può determinare la risoluzione immediata del contratto e l'esclusione dai futuri affidamenti.

Formazione e comunicazione. L'organizzazione garantisce a tutto il personale una formazione anticorruzione iniziale e periodica, differenziata in base al ruolo e al livello di esposizione ai rischi. La presente Politica è comunicata internamente attraverso i canali approvati — e-mail aziendale, Microsoft Teams e sessioni formative — e resa disponibile alle parti interessate esterne mediante il sito web aziendale, i contratti di fornitura e la PEC. I partner commerciali che presentano un rischio di corruzione superiore al livello minimo ricevono comunicazione diretta della Politica.

Autorità e indipendenza della funzione anticorruzione. Il **Responsabile del sistema di gestione**, nella sua veste di funzione di conformità anticorruzione, dispone dell'autorità e dell'indipendenza necessarie per supervisionare il SGAC, con accesso diretto all'Alta Direzione e a tutte le informazioni pertinenti. L'Alta Direzione assicura che tale funzione non subisca interferenze nello svolgimento del proprio mandato.

Archiviazione e aggiornamento

La presente Politica è conservata come informazione documentata all'interno del sistema di gestione documentale dell'organizzazione, sotto la responsabilità del **Responsabile del sistema di gestione**. Il riesame avviene almeno annualmente in occasione del riesame della direzione, oppure a seguito di cambiamenti significativi nel contesto organizzativo, normativo o operativo. Ogni revisione è identificata da un numero progressivo di versione, approvata dall'Alta Direzione e comunicata al personale e alle parti interessate attraverso i canali approvati.

Documenti di riferimento

- Codice di condotta
- PRO Procedura dei ruoli e responsabilità
- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Procedura di due diligence
- PRO Procedura di gestione delle risorse umane
- POL Politica Gestione Conflitto d'interesse
- POL Politica anticorruzione per i partner commerciali
- PRO Procedura di gestione delle segnalazioni
- PRO Procedura gestione dei regali/ donazioni/ sponsorizzazioni

POL Informativa annuale sulla Parità di Genere (PDG)

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Impegno e obiettivi del sistema di gestione sulla parità di genere
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente Politica esprime l'impegno di Tekna S.r.l. a promuovere la parità di genere, prevenire ogni forma di discriminazione diretta o indiretta e garantire pari opportunità di accesso, crescita e valorizzazione per tutte le persone che operano nell'organizzazione, indipendentemente dal genere.

Tekna riconosce nella diversità una risorsa strategica per l'innovazione e la qualità dei servizi di ingegneria erogati nel settore delle infrastrutture di telecomunicazione e dell'ingegneria civile. Con questo documento, l'organizzazione formalizza i principi, gli obiettivi e le responsabilità che orientano l'intero Sistema di Gestione per la Parità di Genere (SGPG), fondato sui valori dell'equità, dell'inclusione e del rispetto reciproco.

La Politica costituisce la base etico-strategica su cui si fondano le azioni definite nel *Piano strategico dell'Organizzazione su tematiche Parità di Genere* e rappresenta una dichiarazione trasparente della volontà dell'organizzazione di perseguire la parità di genere, valorizzare le diversità e supportare l'empowerment femminile, in coerenza con i requisiti della UNI/PdR 125:2022.

Campo di applicazione

La presente Politica si applica alla sede operativa di Tekna S.r.l. in Via Armando Diaz 41, 91025 Marsala (TP), e coinvolge tutto il personale dipendente a tempo indeterminato e determinato, i collaboratori con contratto di co.co.co. e i prestatori d'opera con partita IVA che operano per conto dell'organizzazione. I principi qui espressi riguardano tutti i processi aziendali — direzionali, operativi e di supporto — con particolare riferimento alla gestione delle risorse umane, ai percorsi di carriera, alla comunicazione interna ed esterna, e alle attività di selezione e assunzione del personale.

Riferimenti normativi

- UNI/PdR 125:2022
- D.Lgs. 198/2006
- D.Lgs. 151/2001
- L. 234/2021
- D.Lgs. 105/2022
- D.Lgs. 24/2023
- Direttiva (UE) 2023/970

Termini e definizioni

- **Parità di genere** : condizione in cui donne e uomini godono di pari diritti, responsabilità e opportunità in tutti gli ambiti della vita lavorativa e sociale.

- **Empowerment femminile** : processo di rafforzamento delle competenze, dell'autonomia decisionale e della partecipazione delle donne alla vita economica e organizzativa.
- **Discriminazione diretta** : situazione nella quale una persona è trattata meno favorevolmente di un'altra in ragione del genere, in circostanze comparabili.
- **Discriminazione indiretta** : disposizione, criterio o prassi apparentemente neutri che pongono le persone di un determinato genere in posizione di svantaggio rispetto alle altre.
- **Molestia** : comportamento indesiderato connesso al genere di una persona, avente lo scopo o l'effetto di violarne la dignità e di creare un clima intimidatorio, ostile, degradante, umiliante od offensivo.
- **Conciliazione vita-lavoro** : insieme di misure e strumenti volti a consentire una distribuzione equilibrata del tempo tra responsabilità professionali e personali, indipendentemente dal genere.
- **Comitato Guida** : organo collegiale istituito dall'organizzazione con il compito di indirizzare, monitorare e verificare l'attuazione del Sistema di Gestione per la Parità di Genere.

Ruoli e responsabilità

- **Top Management** : approva la presente Politica, assicura le risorse necessarie all'attuazione del SGPG e delibera le azioni di miglioramento emerse dal riesame annuale.
- **Comitato Guida** : supervisiona l'implementazione del SGPG, verifica la coerenza delle pratiche aziendali con i principi di parità, propone iniziative per il benessere organizzativo e monitora i KPI del Piano Strategico.
- **Responsabile del sistema di gestione** : coordina le attività operative del SGPG, raccoglie e consolida i dati disaggregati per genere, predispone la documentazione per il riesame e cura l'aggiornamento della presente Politica.

Impegno e obiettivi del sistema di gestione sulla parità di genere

Tekna S.r.l. adotta la presente Politica quale dichiarazione del proprio impegno volontario, strutturato e continuativo a favore dell'equità di genere nell'ambiente di lavoro. Tale impegno si articola lungo cinque principi etici fondamentali: imparzialità e inclusività, correttezza e trasparenza, valorizzazione del personale, tutela della persona, contrasto a ogni forma di violenza e discriminazione.

Gestione del personale e delle carriere

L'organizzazione persegue l'equità nei processi di selezione, assunzione e sviluppo professionale. I percorsi di carriera si fondano esclusivamente su criteri documentati di merito — competenze tecniche, risultati progettuali, soft skill e completamento della

formazione — senza alcuna distinzione legata al genere, all'età, all'origine o ad altri fattori non professionali. Tekna promuove l'accesso paritario a ruoli di responsabilità, monitorando annualmente la distribuzione di genere nelle posizioni di coordinamento e verificando l'assenza di divari retributivi non giustificati, con una soglia di attenzione fissata al dieci per cento dello scostamento della retribuzione annua lorda a parità di inquadramento. Le procedure *PRO Procedura per la gestione della carriera*, *PRO Procedura di assunzione e recruiting* e *PRO Procedura equità salariale* traducono questi impegni in criteri operativi e indicatori misurabili.

Conciliazione vita-lavoro e supporto alla genitorialità

Tekna riconosce il diritto di ogni persona a un equilibrio sostenibile tra responsabilità professionali e vita personale. A tal fine l'organizzazione adotta misure concrete di flessibilità oraria, con fascia di presenza obbligatoria dalle 9:00 alle 13:00 e possibilità di ingresso tra le 8:00 e le 10:00, lavoro da remoto per attività compatibili, contratti part-time accessibili senza discriminazioni di genere o ruolo e un programma di welfare che prevede il rimborso delle utenze domestiche differenziato per situazione familiare. A sostegno della genitorialità, l'organizzazione garantisce il pieno esercizio dei congedi di maternità, paternità e parentali, promuove attivamente il congedo di paternità obbligatorio e offre un piano di rientro personalizzato dopo il congedo, comprensivo di formazione di aggiornamento e affiancamento. Le procedure *PRO Procedura work-life balance* e *PRO Procedura supporto alla genitorialità* disciplinano nel dettaglio le modalità di accesso e gestione di queste misure.

Prevenzione delle molestie e tutela della dignità

L'organizzazione adotta una posizione di tolleranza zero verso ogni forma di molestia, violenza, discriminazione o abuso di potere nei rapporti di lavoro, siano essi di natura fisica, verbale, sessuale, psicologica o digitale. Tekna promuove una cultura del rispetto attraverso la formazione periodica di tutto il personale, la valutazione annuale del clima lavorativo e l'istituzione di un canale di segnalazione anonimo accessibile a chiunque operi nell'organizzazione, garantendo riservatezza, imparzialità e protezione del segnalante da qualsiasi ritorsione. Il *Regolamento per contrastare molestie e abusi* e la *PRO Procedura per la prevenzione delle molestie sul luogo di lavoro* definiscono le misure preventive, i flussi di gestione dei reclami e le relative sanzioni.

Comunicazione inclusiva

Tekna si impegna affinché la comunicazione interna ed esterna — inclusa ogni forma di presentazione commerciale, bando di selezione e materiale informativo — adotti un linguaggio inclusivo e privo di stereotipi di genere. Gli annunci di ricerca del personale sono redatti in forma neutra rispetto al genere e sottoposti alla verifica del Comitato Guida prima della pubblicazione, conformemente a quanto previsto dalla *PRO Procedura di assunzione e recruiting*. La *PRO Procedura gestione comunicazione* disciplina i canali e le modalità attraverso cui l'organizzazione rende accessibili le informazioni sulla parità di genere a tutte le parti interessate, interne ed esterne.

Valorizzazione delle diversità e empowerment femminile

Consapevole della sottorappresentazione femminile nel settore dell'ingegneria civile e delle telecomunicazioni, Tekna promuove azioni proporzionate alla propria dimensione organizzativa per favorire la crescita professionale delle donne: percorsi formativi in materia di leadership, partecipazione a eventi di settore e affiancamento interno da parte di figure senior. Il Comitato Guida definisce obiettivi progressivi di equilibrio di genere, verificandone l'avanzamento in sede di riesame annuale del SGPG.

Obiettivi del sistema di gestione

L'organizzazione persegue i seguenti obiettivi attraverso il proprio SGPG:

- garantire la trasparenza e la misurabilità delle azioni intraprese, attraverso la raccolta sistematica di dati disaggregati per genere su assunzioni, cessazioni, inquadramenti, accesso alla formazione e utilizzo di misure di flessibilità;
- promuovere condizioni di lavoro che favoriscano il benessere e la produttività di tutte le persone, indipendentemente dal genere;
- monitorare annualmente gli indicatori di parità e inclusione, confrontandoli con gli obiettivi del Piano Strategico e attivando azioni correttive in caso di scostamenti significativi;
- assicurare il miglioramento continuo del SGPG mediante il riesame periodico della Direzione, condotto almeno una volta l'anno con il coinvolgimento del Comitato Guida e del **Responsabile del sistema di gestione**.

Archiviazione e aggiornamento

La presente Politica è conservata nel sistema documentale aziendale con classificazione di riservatezza "limited" ed è accessibile a tutto il personale mediante i canali di comunicazione interna. Il **Responsabile del sistema di gestione** ne cura la revisione almeno annuale, in occasione del riesame del SGPG da parte della Direzione, oppure ogni volta che intervengano modifiche normative, organizzative o di contesto rilevanti. Ogni aggiornamento è sottoposto all'approvazione del Top Management e comunicato a tutti i destinatari interni ed esterni entro trenta giorni dalla pubblicazione.

Documenti di riferimento

- Piano strategico dell'Organizzazione su tematiche Parità di Genere
- Codice etico aziendale
- Piano di welfare aziendale
- Regolamento del Comitato Guida
- Regolamento per contrastare molestie e abusi
- PRO Procedura per la gestione della carriera
- PRO Procedura di assunzione e recruiting

- PRO Procedura equità salariale
- PRO Procedura work-life balance
- PRO Procedura supporto alla genitorialità
- PRO Procedura per la prevenzione delle molestie sul luogo di lavoro
- PRO Procedura gestione comunicazione
- PRO Revisione periodica del Sistema Parità di Genere

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Protezione degli asset fuori sede
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica dichiara e comunica l'impegno del Top Management di Tekna S.r.l. verso la protezione degli asset informativi dell'organizzazione. Attraverso questo documento, l'azienda definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI), orientandolo alla salvaguardia della riservatezza, dell'integrità e della disponibilità delle informazioni che sostengono l'erogazione dei servizi di ingegneria civile e impiantistica, di consulenza tecnica ambientale e di progettazione per le telecomunicazioni.

Il Top Management riconosce che la sicurezza delle informazioni è un fattore abilitante per la fiducia dei committenti — in particolare degli operatori di telecomunicazioni e dei soggetti che affidano incarichi nell'ambito di gare pubbliche e private — e per la continuità operativa dell'organizzazione nel suo complesso. La presente politica costituisce pertanto il documento apicale del SGSI e fornisce la cornice entro cui si sviluppano tutte le politiche specifiche e le procedure operative di sicurezza delle informazioni.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi — in formato digitale, cartaceo o di qualsiasi altra natura — e ai sistemi tecnologici gestiti dall'organizzazione nella sede operativa di Via Armando Diaz 41, Marsala (TP). Essa coinvolge tutto il personale dipendente, i collaboratori a partita IVA, i consulenti e le terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità e dal luogo di svolgimento della prestazione.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza** : proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.

- **Rischio** : effetto dell'incertezza sugli obiettivi.
- **Asset** : qualsiasi elemento che abbia valore per l'organizzazione, incluse informazioni, software, hardware, infrastrutture fisiche, servizi, persone e beni immateriali.
- **Evento di sicurezza delle informazioni** : occorrenza identificata relativa a un sistema, servizio o rete, che indica una possibile violazione della politica di sicurezza delle informazioni, un guasto dei controlli o una situazione precedentemente sconosciuta che può essere rilevante per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità di compromettere le operazioni e di minacciare la sicurezza delle informazioni.

Ruoli e responsabilità

- **Top Management** : approva la presente politica, ne garantisce l'adeguatezza rispetto al contesto aziendale e assicura le risorse necessarie al funzionamento efficace del SGSI.
- **Responsabile del sistema di gestione** : sovrintende all'attuazione, al monitoraggio e al miglioramento continuo del SGSI, curando il riesame periodico della presente politica e coordinando la comunicazione interna ed esterna in materia di sicurezza delle informazioni.

Obiettivi di sicurezza delle informazioni

Tekna S.r.l. persegue obiettivi di sicurezza delle informazioni coerenti con la propria strategia aziendale e con i risultati della valutazione dei rischi. In particolare l'organizzazione si impegna a:

- Preservare la riservatezza delle informazioni dei committenti — in primo luogo degli operatori di telecomunicazioni — e dei dati personali trattati nell'ambito delle proprie attività.
- Garantire l'integrità della documentazione tecnica di progetto, delle relazioni di collaudo e delle misurazioni ambientali (campi elettromagnetici, fonometria), affinché i risultati mantengano accuratezza e attendibilità lungo l'intero ciclo di vita del servizio.
- Assicurare la disponibilità dei sistemi informativi e delle piattaforme operative utilizzate per la gestione delle commesse e la comunicazione con clienti e fornitori, minimizzando i tempi di indisponibilità e prevenendo la perdita di dati critici.
- Promuovere la consapevolezza di tutto il personale — dipendente, collaboratore e terza parte autorizzata — riguardo alle minacce alla sicurezza delle informazioni e alle corrette prassi di protezione.
- Soddisfare i requisiti normativi, contrattuali e regolamentari applicabili in materia di protezione dei dati e sicurezza delle informazioni.
- Migliorare continuamente l'efficacia del SGSI attraverso il monitoraggio degli indicatori di prestazione, l'analisi degli incidenti e il riesame della direzione.

Principi fondamentali di sicurezza delle informazioni

L'organizzazione fonda il proprio SGSI su un insieme di principi che permeano ogni politica, procedura e controllo operativo adottato a tutela degli asset informativi.

Approccio basato sul rischio. Tekna S.r.l. adotta un metodo sistematico di identificazione, valutazione e trattamento dei rischi per la sicurezza delle informazioni, calibrato sul proprio contesto operativo e sulla tipologia di dati trattati. Le decisioni in materia di protezione derivano dall'analisi di probabilità e impatto delle minacce rilevate, e i controlli sono proporzionati al livello di rischio residuo accettato dal Top Management.

Responsabilità condivisa. La sicurezza delle informazioni non è prerogativa esclusiva di una singola funzione: tutto il personale, i collaboratori e le terze parti autorizzate contribuiscono attivamente alla protezione degli asset informativi nel proprio ambito di competenza. L'assegnazione formale dei beni aziendali a ciascun assegnatario comporta l'impegno alla custodia, all'uso accettabile e alla restituzione al termine del rapporto.

Classificazione e protezione delle informazioni. L'organizzazione classifica le proprie informazioni in base alla sensibilità e ai requisiti di protezione — distinguendo i livelli pubblico, limitato e riservato — e adotta misure di trattamento, trasmissione e conservazione commisurate a ciascun livello, garantendo che l'etichettatura renda visibile la classificazione adottata.

Uso accettabile delle risorse. Ogni risorsa informativa — sistema, dispositivo, software, dato — è utilizzata esclusivamente per finalità aziendali autorizzate, nel rispetto delle regole stabilite dalla *POL Politica di sicurezza operativa* e dalla *POL Politica di classificazione ed etichettatura delle informazioni*. L'organizzazione documenta gli utenti autorizzati e i relativi diritti di accesso attraverso il *Registro degli utenti autorizzati all'uso delle informazioni*.

Scrivania pulita e schermo pulito. L'organizzazione promuove regole chiare per evitare l'esposizione non autorizzata di informazioni sensibili: i documenti cartacei classificati come limitati o riservati non rimangono incustoditi sulle postazioni di lavoro, e i dispositivi attivano il blocco automatico dello schermo dopo un periodo di inattività, così da prevenire l'accesso fisico non autorizzato alle informazioni visualizzate.

Segnalazione tempestiva degli eventi di sicurezza. L'organizzazione mette a disposizione del personale canali dedicati per la comunicazione immediata di ogni evento — osservato o sospetto — che possa costituire una violazione della sicurezza delle informazioni. La segnalazione tempestiva è un obbligo individuale che consente l'attivazione rapida delle procedure di risposta agli incidenti, come disciplinato dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* e registrato nel *MOD Registro degli incidenti di sicurezza delle informazioni*.

Conformità normativa e contrattuale. Tekna S.r.l. si impegna a identificare, rispettare e tenere aggiornato il quadro degli obblighi legali, regolamentari e contrattuali applicabili alla sicurezza delle informazioni, includendo la normativa sulla protezione dei dati personali e gli impegni assunti verso i committenti in sede contrattuale.

Miglioramento continuo. Il Top Management promuove il riesame periodico del SGSI, l'analisi degli esiti degli audit interni ed esterni, il monitoraggio degli indicatori di

prestazione e l'apprendimento derivante dagli incidenti, al fine di adeguare costantemente i controlli all'evoluzione del contesto tecnologico, organizzativo e delle minacce.

Protezione degli asset fuori sede

L'organizzazione riconosce che le proprie informazioni e i dispositivi che le contengono richiedono protezione anche quando operano al di fuori della sede di Via Armando Diaz 41, Marsala. Questa esigenza è particolarmente rilevante per il personale tecnico impegnato in sopralluoghi presso cantieri, siti di telecomunicazione e sedi dei committenti, nonché per gli strumenti di misura assegnati in comodato.

Tekna S.r.l. si impegna a garantire che ogni asset fuori sede — notebook, dispositivi mobili, strumenti di misura, supporti rimovibili e documenti cartacei trasportati per esigenze operative — mantenga un livello di protezione equivalente a quello assicurato all'interno dei locali aziendali, attraverso i seguenti principi:

- **Custodia** : gli asset non sono lasciati incustoditi in veicoli, mezzi pubblici, aree comuni di strutture ricettive o spazi di coworking. In trasferta vengono custoditi in luogo chiuso a chiave sotto la responsabilità dell'assegnatario.
- **Trasporto** : ogni bene è trasportato in custodia personale dall'assegnatario. Per le consegne a consulenti, fornitori o sedi distaccate l'organizzazione privilegia canali tracciati.
- **Segnalazione di smarrimento, furto o danneggiamento** : il personale comunica immediatamente al **Responsabile del sistema di gestione** qualunque smarrimento, furto o danneggiamento di asset aziendali fuori sede. Tale comunicazione innesca l'attivazione delle misure di blocco remoto del dispositivo, la revoca degli accessi e la sostituzione delle credenziali; l'evento è registrato come incidente di sicurezza delle informazioni nel *MOD Registro degli incidenti di sicurezza delle informazioni* .
- **Restituzione** : al termine della trasferta, del progetto o del rapporto di collaborazione, l'asset è restituito all'organizzazione con le modalità previste dal *MOD Modulo di assegnazione dei beni* .

Per il lavoro a distanza, l'organizzazione prescrive che i dispositivi utilizzati per accedere alla rete aziendale siano conformi ai requisiti definiti nella *POL Politica di sicurezza operativa* , prevedendo in particolare l'installazione di software antivirus aggiornato, l'utilizzo esclusivo di strumenti di accesso remoto forniti dall'azienda con autenticazione a più fattori, e il rispetto delle regole di scrivania pulita anche nell'ambiente domestico o esterno.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI. Il **Responsabile del sistema di gestione** ne cura l'archiviazione secondo le modalità definite dalla *PRO Procedura di gestione delle informazioni documentate* e ne assicura la disponibilità a tutto il personale interessato. Il riesame avviene con cadenza annuale, in occasione del riesame della direzione, oppure a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia, nel quadro normativo o nel panorama delle minacce. Ogni modifica approvata dal Top Management comporta l'aggiornamento dell'indice di revisione e la comunicazione

a tutte le parti interessate, interne ed esterne, secondo le prassi di diffusione delle politiche del sistema di gestione.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- MOD Registro degli incidenti di sicurezza delle informazioni
- MOD Modulo di assegnazione dei beni
- Registro degli utenti autorizzati all'uso delle informazioni

POL Politica di sicurezza operativa

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Backup
- Protezione dei dati personali
- Gestione dei log
- Uso accettabile delle informazioni e degli asset
- Bring Your Own Device (BYOD)
- Protezione delle informazioni fuori sede
- Controlli fisici della postazione remota
- Controlli sulla rete domestica
- Canali di comunicazione sicuri
- Revoca degli accessi al termine del rapporto o cambio ruolo
- Utilizzo dei servizi cloud
- Utilizzo dei supporti di memorizzazione rimovibili
- Scrivania e schermo puliti
- Gestione delle capacità
- Gestione delle vulnerabilità
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica esprime l'impegno di Tekna S.r.l. a garantire il funzionamento corretto, sicuro e resiliente dei propri sistemi di elaborazione delle informazioni, delle reti e dell'infrastruttura IT a supporto delle attività di ingegneria e consulenza tecnica nel settore delle telecomunicazioni e delle energie rinnovabili. L'organizzazione riconosce che la protezione della riservatezza, dell'integrità e della disponibilità delle informazioni durante le operazioni quotidiane costituisce un requisito imprescindibile per la continuità del servizio e la fiducia dei propri committenti.

Attraverso questo documento, Tekna promuove un approccio strutturato alla sicurezza operativa che abbraccia la gestione dei backup, la registrazione e il monitoraggio degli eventi, il controllo delle vulnerabilità tecniche, la gestione dei cambiamenti e l'uso responsabile delle risorse informative. La politica persegue la riduzione al minimo dei rischi di interruzione, perdita di dati e incidenti di sicurezza, integrando tali obiettivi nelle prassi operative dell'intera organizzazione.

Campo di applicazione

La presente politica si applica a tutto il personale di Tekna S.r.l. — dipendenti, collaboratori e consulenti — operante presso la sede di Via Armando Diaz 41, 91025 Marsala (TP) e presso i siti di progetto o le sedi dei committenti. Rientrano nel campo di applicazione tutti i sistemi di elaborazione delle informazioni, i dispositivi endpoint, le infrastrutture di rete, i servizi cloud utilizzati dall'organizzazione, i supporti di memorizzazione e le informazioni in formato digitale e cartaceo gestite nell'ambito dei servizi di ingegneria per telecomunicazioni e infrastrutture civili. Sono esclusi gli ambienti di sviluppo software, disciplinati dalla *PRO Procedura di sviluppo sicuro*.

Riferimenti normativi

- ISO/IEC 27001:2022
- Regulation (EU) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Backup** : copia di dati, software o configurazioni di sistema conservata a fini di ripristino in caso di perdita, corruzione o indisponibilità dell'originale.
- **Log** : registrazione cronologica di eventi, attività, eccezioni o guasti generati da sistemi, applicazioni o dispositivi di rete.
- **Vulnerabilità tecnica** : debolezza di un asset o di un controllo che può essere sfruttata da una o più minacce.

- **Supporto di memorizzazione rimovibile** : dispositivo fisico portatile utilizzato per archiviare o trasferire dati, quali unità USB, dischi esterni o supporti ottici.
- **Endpoint** : dispositivo utente finale — computer portatile, workstation, tablet o smartphone — che accede alle risorse informative dell'organizzazione.
- **Gestione del cambiamento** : insieme di attività volte a controllare le modifiche alle strutture di elaborazione delle informazioni e ai sistemi informativi, al fine di minimizzare gli impatti negativi sulla sicurezza.
- **Segregazione della rete** : separazione logica o fisica di gruppi di servizi, utenti o sistemi all'interno dell'infrastruttura di rete, volta a contenere la propagazione delle minacce.

Ruoli e responsabilità

- **Responsabile del sistema di gestione** : assicura l'attuazione, il monitoraggio e l'aggiornamento dei controlli operativi di sicurezza definiti dalla presente politica, verificandone la conformità attraverso audit periodici e il riesame delle evidenze.

Backup

Tekna riconosce nella disponibilità delle informazioni un presupposto essenziale per la continuità delle proprie attività di ingegneria e progettazione. L'organizzazione adotta pertanto una strategia di backup che tutela i dati aziendali, i documenti di progetto e le configurazioni dei sistemi critici contro eventi di perdita, corruzione o indisponibilità accidentale.

L'impegno dell'organizzazione si articola nei seguenti principi:

- Tutti i dati operativi e progettuali archiviati nel NAS aziendale sono sottoposti a sincronizzazione periodica settimanale verso un server di backup dedicato, con volume di destinazione cifrato per garantire la riservatezza anche in caso di accesso fisico non autorizzato.
- Una seconda copia di ridondanza viene generata su base mensile per assicurare un ulteriore livello di protezione rispetto a eventi che compromettano la copia primaria.
- I backup sono verificati regolarmente attraverso test di ripristino, al fine di accertare l'effettiva recuperabilità dei dati entro i tempi richiesti dalla continuità del servizio.
- Il periodo di conservazione e il numero di versioni mantenute sono definiti in funzione delle esigenze operative e dei requisiti di ripristino, in modo da bilanciare la profondità storica con l'efficienza delle risorse di archiviazione.

L'organizzazione si impegna a riesaminare periodicamente l'adeguatezza della politica di backup, considerando l'evoluzione del volume di dati, i requisiti contrattuali dei committenti e le risultanze dell'analisi dei rischi. Le modalità operative di esecuzione, conservazione e test dei backup sono dettagliate nella *PRO Procedura di continuità operativa e di ripristino di emergenza*.

Protezione dei dati personali

Tekna si impegna a identificare e soddisfare tutti i requisiti relativi alla tutela della privacy e alla protezione dei dati personali (PII), in conformità al GDPR e alla normativa nazionale applicabile. Tale impegno si traduce nell'adozione di principi di liceità, minimizzazione, limitazione delle finalità e integrità dei trattamenti, integrati in ogni processo operativo che implichi la raccolta, l'elaborazione o la conservazione di dati riferibili a persone fisiche.

L'organizzazione classifica le informazioni personali al livello di riservatezza più elevato previsto dal proprio sistema di classificazione e ne protegge la conservazione mediante controlli di accesso rigorosi, cifratura dei supporti e dei canali di trasmissione, e misure di protezione fin dalla progettazione di ogni nuovo sistema o servizio. L'accesso ai dati personali avviene esclusivamente sulla base del principio di necessità, con identificazione univoca dell'utente e tracciabilità delle operazioni.

Tekna garantisce ai soggetti interessati l'esercizio dei diritti previsti dalla normativa — accesso, rettifica, cancellazione — attraverso procedure documentate e tempi di riscontro definiti, e si impegna a notificare eventuali violazioni dei dati all'autorità di controllo competente nei termini di legge. Le registrazioni relative ai trattamenti effettuati sono conservate e protette da perdita, distruzione o alterazione, in linea con la *POL Politica di protezione delle PII* e con la *POL Politica di conservazione e cancellazione delle informazioni*.

Gestione dei log

L'organizzazione promuove una cultura del monitoraggio continuo, nella convinzione che la tempestiva rilevazione di anomalie e la tracciabilità degli eventi costituiscano la prima linea di difesa contro gli incidenti di sicurezza. Tekna adotta pertanto un sistema strutturato di registrazione, protezione e analisi dei log prodotti dai propri sistemi informativi.

Registrazione degli eventi

Tutti i dispositivi e le applicazioni critiche — inclusi i sistemi di archiviazione, i dispositivi di rete e le soluzioni di protezione endpoint — generano registrazioni che documentano attività degli utenti, eccezioni, guasti e rilevamenti di sicurezza. Le informazioni registrate comprendono, ove tecnicamente possibile, la data e l'ora dell'evento, l'identificativo dell'utente, il tipo e l'esito dell'azione, nonché l'oggetto coinvolto.

Sincronizzazione dell'orologio

Per consentire la correlazione affidabile degli eventi tra sistemi diversi e supportare le indagini sugli incidenti, l'organizzazione mantiene gli orologi di tutti i sistemi di elaborazione sincronizzati con una fonte oraria esterna riconosciuta, garantendo coerenza temporale nelle registrazioni.

Monitoraggio e notifiche

L'organizzazione si impegna a monitorare reti, sistemi e applicazioni per individuare comportamenti anomali e a valutare tempestivamente i potenziali incidenti di sicurezza. I sistemi di backup e di protezione dei dati sono configurati per inviare notifiche automatiche via posta elettronica al personale incaricato della risposta agli incidenti, in modo che ogni variazione di stato o anomalia venga segnalata senza ritardo.

Protezione e conservazione

I log sono protetti da accessi non autorizzati e da alterazioni, al fine di preservarne il valore probatorio. I periodi di conservazione rispondono ai requisiti normativi e alle esigenze di indagine, e la loro revisione periodica assicura che le registrazioni rimangano adeguate, complete e utili alla valutazione della postura di sicurezza dell'organizzazione.

Uso accettabile delle informazioni e degli asset

Tekna riconosce che l'uso responsabile delle risorse informative e degli asset aziendali è condizione necessaria per la tutela del patrimonio informativo e per il rispetto degli obblighi verso i committenti. L'organizzazione definisce pertanto regole chiare, documentate e comunicate a tutto il personale, volte a garantire che informazioni, sistemi, dispositivi e software siano impiegati esclusivamente per le finalità istituzionali e nel rispetto della classificazione attribuita.

Principi generali

L'assegnazione degli asset avviene in modo formale e tracciato attraverso il *MOD Modulo di assegnazione dei beni*, che vincola l'assegnatario alla custodia, all'uso conforme e alla restituzione al termine del rapporto. L'organizzazione mantiene un *Registro degli utenti autorizzati all'uso delle informazioni* nel quale ogni utente è associato ai sistemi, alle repository e alle informazioni cui ha legittimamente accesso, in modo da garantire il principio di necessità.

Protezione contro malware

L'organizzazione adotta soluzioni anti-malware su tutti i dispositivi endpoint, con aggiornamento automatico delle definizioni e scansioni periodiche. Tutto il personale è tenuto a non disattivare o aggirare le protezioni attive, a non aprire allegati o collegamenti di origine sospetta e a segnalare tempestivamente qualsiasi comportamento anomalo del sistema.

Installazione del software

L'installazione di nuovo software sui dispositivi aziendali è riservata esclusivamente al personale espressamente designato. Ogni richiesta di installazione deve essere motivata e autorizzata prima dell'esecuzione; sono consentiti a tutto il personale unicamente gli aggiornamenti di sicurezza e le patch del software già presente. L'organizzazione mantiene un monitoraggio delle applicazioni installate per prevenire l'introduzione di software non approvato.

Programmi di utilità privilegiati

L'uso di programmi di utilità capaci di aggirare i controlli del sistema operativo o delle applicazioni è strettamente limitato al personale con responsabilità amministrative sui sistemi, con accesso riconducibile a identità univoche. L'organizzazione vieta l'utilizzo di tali strumenti per finalità diverse dalla manutenzione e dall'amministrazione autorizzata, e ne documenta ogni impiego significativo.

Procedure operative documentate

Tutte le procedure operative per le strutture di elaborazione delle informazioni sono documentate, rese accessibili al personale coinvolto e aggiornate in occasione di cambiamenti significativi. L'organizzazione promuove la diffusione interna delle politiche e

delle istruzioni attraverso i canali di comunicazione stabiliti, affinché ogni collaboratore conosca i propri obblighi operativi in materia di sicurezza.

Bring Your Own Device (BYOD)

Tekna adotta un approccio prudente all'utilizzo di dispositivi personali per finalità lavorative, consapevole che l'impiego di apparecchiature non gestite dall'organizzazione introduce rischi aggiuntivi per la riservatezza e l'integrità delle informazioni aziendali. L'uso di dispositivi personali per accedere a dati o sistemi aziendali è consentito esclusivamente previa autorizzazione formale e nel rispetto dei requisiti minimi di sicurezza definiti dall'organizzazione.

I dispositivi personali ammessi al trattamento di informazioni aziendali devono garantire l'aggiornamento costante del sistema operativo e delle protezioni anti-malware, il blocco automatico in caso di inattività, la cifratura dei dati memorizzati localmente e l'assenza di software non conforme alle politiche aziendali. L'organizzazione si riserva la facoltà di verificare il rispetto di tali requisiti e di revocare l'autorizzazione qualora le condizioni di sicurezza non siano mantenute.

È vietato archiviare informazioni classificate come riservate su dispositivi personali o su servizi cloud non approvati. Al termine del rapporto di collaborazione o in caso di revoca dell'autorizzazione, il personale è tenuto a rimuovere ogni dato aziendale dal proprio dispositivo.

Protezione delle informazioni fuori sede

Le informazioni aziendali accedute, elaborate o conservate al di fuori della sede di Marsala — in particolare durante i sopralluoghi tecnici, le attività presso cantieri e le visite ai committenti nel settore telecomunicazioni e infrastrutture — devono essere protette da perdita, furto e accesso non autorizzato con lo stesso livello di garanzia assicurato in sede.

Il personale operante fuori sede utilizza esclusivamente dispositivi assegnati dall'organizzazione o approvati nell'ambito del programma BYOD, e adotta le seguenti misure di protezione:

- Non lasciare incustoditi dispositivi contenenti dati aziendali, in particolare presso cantieri, mezzi di trasporto o aree ad accesso pubblico.
- Attivare il blocco dello schermo in caso di inattività, anche per brevi allontanamenti.
- Custodire i documenti fisici contenenti informazioni classificate come riservate o limitate in modo sicuro e provvedere alla loro distruzione adeguata al termine dell'utilizzo.

L'organizzazione promuove la consapevolezza del personale rispetto ai rischi specifici connessi al lavoro fuori sede, integrando tali aspetti nelle attività di informazione e formazione periodica sulla sicurezza delle informazioni.

Controlli fisici della postazione remota

Qualora il personale operi occasionalmente da una postazione diversa dalla sede aziendale, l'organizzazione richiede l'adozione di misure fisiche idonee a prevenire la visualizzazione delle informazioni da parte di persone non autorizzate e l'accesso indebito ai dispositivi.

L'area di lavoro deve essere allestita in modo da impedire la visione dello schermo a terzi non autorizzati. I dispositivi aziendali non possono essere lasciati incustoditi in luoghi pubblici o all'interno di veicoli, e l'accesso fisico alla postazione deve essere limitato alle sole persone che ne abbiano legittimo titolo. Al termine della sessione di lavoro, le informazioni aziendali visualizzate o stampate devono essere riposte o eliminate in modo sicuro.

Controlli sulla rete domestica

L'organizzazione riconosce che l'accesso alle risorse aziendali da reti esterne alla sede comporta rischi aggiuntivi di intercettazione e accesso non autorizzato. Nei casi in cui il personale debba accedere ai sistemi interni da una rete diversa da quella aziendale, l'organizzazione stabilisce i seguenti principi:

- L'accesso ai sistemi e alle applicazioni interne avviene tramite connessione protetta da protocolli di cifratura adeguati.
- Il personale è tenuto ad assicurare che la propria rete di connessione utilizzi protocolli di cifratura aggiornati e credenziali personalizzate, evitando la trasmissione di informazioni riservate su reti non protette.
- L'organizzazione si impegna a rendere disponibili strumenti e configurazioni che consentano connessioni sicure anche al di fuori della sede, tutelando l'integrità e la riservatezza delle comunicazioni.

Tali misure si applicano in via prioritaria a qualunque attività che implichi l'accesso a dati classificati come riservati o limitati.

Canali di comunicazione sicuri

Tekna si impegna a garantire che tutte le comunicazioni riguardanti informazioni aziendali riservate avvengano attraverso canali approvati dall'organizzazione, idonei a preservare la riservatezza e l'integrità dei contenuti trasmessi.

L'utilizzo di applicazioni di messaggistica personale o di account di posta elettronica non aziendali per la trasmissione di informazioni classificate come riservate o limitate è vietato. Le videoconferenze che trattano argomenti sensibili devono essere protette da credenziali di accesso e condotte in ambienti che garantiscano la riservatezza della comunicazione, in coerenza con i controlli fisici della postazione.

L'organizzazione individua e comunica al personale l'elenco dei canali e degli strumenti approvati, aggiornandolo in funzione dell'evoluzione tecnologica e delle risultanze dell'analisi dei rischi.

Revoca degli accessi al termine del rapporto o cambio ruolo

L'organizzazione si impegna a revocare tempestivamente gli accessi logici e fisici del personale in uscita o soggetto a cambio di ruolo, al fine di prevenire l'utilizzo non autorizzato delle risorse informative. Tale principio si applica a tutte le tipologie di rapporto — dipendenti, collaboratori e consulenti — e a tutti i sistemi in uso, inclusi i servizi cloud, i portali dei committenti e gli archivi di rete.

La revoca avviene entro ventiquattro ore dalla cessazione del rapporto o dalla comunicazione del cambio di mansione. In caso di interruzione immediata per giusta causa, la disattivazione degli account è eseguita contestualmente alla comunicazione del provvedimento. Il personale in uscita è tenuto alla restituzione di tutti i dispositivi aziendali assegnati e alla rimozione di qualsiasi informazione aziendale eventualmente presente su dispositivi personali.

In presenza di cambio di ruolo senza cessazione del rapporto, i diritti di accesso vengono riesaminati alla luce delle nuove responsabilità e adeguati secondo il principio del minimo privilegio. Le modalità operative di deprovisioning sono disciplinate nella *PRO Procedura di gestione e controllo degli accessi logici*.

Utilizzo dei servizi cloud

Tekna utilizza servizi cloud di terze parti a supporto delle proprie attività gestionali e di collaborazione, consapevole che l'adozione di tali servizi richiede un governo attento dei rischi connessi alla riservatezza, all'integrità e alla disponibilità delle informazioni affidate a infrastrutture esterne. L'organizzazione adotta i seguenti principi per l'acquisizione, l'utilizzo e la gestione dei servizi cloud:

- L'attivazione di un nuovo servizio cloud richiede l'autorizzazione di una funzione responsabile e una valutazione preventiva dei termini contrattuali, dei requisiti di protezione dei dati e delle garanzie di sicurezza offerte dal fornitore, in coerenza con la *PRO Procedura di gestione degli acquisti e delle terze parti*.
- I servizi cloud autorizzati sono censiti nell'elenco dei fornitori qualificati con indicazione della criticità e delle tipologie di dati trattati.
- L'organizzazione si impegna a verificare periodicamente che le condizioni contrattuali dei servizi in uso non siano mutate in modo significativo e che i livelli di sicurezza restino adeguati.
- I fornitori di servizi ICT critici sono tenuti a comunicare preventivamente eventuali variazioni dei sub-fornitori coinvolti nel trattamento dei dati dell'organizzazione.

Segregazione della rete

L'organizzazione applica una separazione logica della propria infrastruttura di rete allo scopo di contenere la propagazione delle minacce e di isolare i flussi informativi in base alla loro criticità e funzione. La rete aziendale è strutturata in segmenti distinti, ciascuno con un livello di accesso appropriato:

- Una rete interna a disposizione del personale autorizzato, con accesso ai sistemi di archiviazione, ai dispositivi di stampa e alle applicazioni operative.
- Una rete separata per gli ospiti e per i dispositivi non gestiti, isolata dalla rete interna e con accesso limitato alla connettività Internet.

Il traffico tra i segmenti di rete è controllato dal firewall aziendale secondo il principio di default-deny: soltanto i flussi esplicitamente necessari e autorizzati sono consentiti. Le configurazioni dei dispositivi di rete sono protette da credenziali amministrative dedicate e soggette a revisione periodica per rimuovere regole obsolete o non più giustificate.

L'organizzazione si impegna a mantenere aggiornato il diagramma di rete — documentato nel *MOD Diagramma di rete* — quale riferimento per la pianificazione della sicurezza, la gestione dei cambiamenti e la verifica della conformità. Le modalità operative di configurazione, hardening e manutenzione dell'infrastruttura di rete sono disciplinate nella *PRO Procedura di gestione della sicurezza della rete*.

Utilizzo dei supporti di memorizzazione rimovibili

L'organizzazione adotta un approccio restrittivo all'uso dei supporti di memorizzazione rimovibili, riconoscendo che tali dispositivi — unità USB, dischi esterni, supporti ottici — rappresentano un vettore significativo di rischio per la fuoriuscita non controllata di informazioni e per l'introduzione di malware nell'ambiente aziendale.

L'utilizzo di supporti rimovibili è consentito esclusivamente nei casi in cui risulti strettamente necessario dal punto di vista operativo e previa autorizzazione del **Responsabile del sistema di gestione**. I supporti contenenti informazioni classificate come riservate o limitate devono essere cifrati, custoditi in ambienti ad accesso controllato e mai lasciati incustoditi in aree comuni o pubbliche. Il trasporto fisico avviene sotto la diretta custodia del personale autorizzato e ogni trasferimento è registrato con indicazione del supporto, del mittente, del destinatario, della data e della cifratura applicata.

È vietato l'uso di supporti rimovibili non cifrati per informazioni riservate. I supporti devono recare un'etichetta che identifichi il livello massimo di classificazione delle informazioni contenute. Lo smaltimento dei supporti al termine del ciclo di vita avviene secondo modalità che impediscano il recupero dei dati, anche con mezzi forensi, in conformità alla *PRO Procedura di configurazione, gestione e smaltimento degli asset*.

Scrivania e schermo puliti

Tekna promuove l'adozione sistematica di regole di scrivania pulita e schermo pulito, nella convinzione che la protezione delle informazioni inizi dal controllo dell'ambiente fisico di lavoro e dalla prevenzione dell'esposizione involontaria di dati.

Al termine dell'attività lavorativa e durante le assenze dalla postazione, i documenti cartacei contenenti informazioni classificate come riservate o limitate devono essere riposti in contenitori chiusi o in aree ad accesso controllato. Le scrivanie non devono presentare informazioni sensibili visibili a terzi non autorizzati, inclusi post-it con credenziali, stampe di progetto e documentazione tecnica dei committenti.

I dispositivi aziendali sono configurati per attivare automaticamente il blocco dello schermo dopo un periodo di inattività prestabilito. Il personale è tenuto ad attivare manualmente il blocco ogni volta che si allontana dalla postazione, anche per brevi interruzioni. Nessuna informazione classificata deve restare visibile su schermi incustoditi, né in sede né presso cantieri o sedi dei committenti.

Gestione delle capacità

L'organizzazione si impegna a monitorare le risorse dei propri sistemi di elaborazione affinché la capacità disponibile rimanga costantemente allineata ai requisiti operativi correnti e prevedibili. L'obiettivo è prevenire il degrado delle prestazioni e l'indisponibilità dei servizi derivanti dal raggiungimento dei limiti di capacità.

Il monitoraggio comprende i parametri critici dell'infrastruttura — capacità di archiviazione, utilizzo della CPU, memoria e indicatori ambientali dei dispositivi — e si estende ai servizi cloud in uso, per i quali l'organizzazione verifica l'adeguatezza dei piani sottoscritti rispetto all'evoluzione delle necessità.

Al rilevamento di un avvicinamento alle soglie critiche, l'organizzazione valuta e attua le misure di adeguamento necessarie — ampliamento delle risorse, ottimizzazione dello spazio o migrazione a soluzioni più adeguate — con tempistiche proporzionate alla criticità del servizio interessato. Il **Responsabile del sistema di gestione** riesamina periodicamente i dati di utilizzo, ne valuta le tendenze e integra le risultanze nel riesame della direzione quale elemento di pianificazione delle risorse.

Gestione delle vulnerabilità

Tekna adotta un approccio proattivo all'identificazione e al trattamento delle vulnerabilità tecniche dei propri sistemi informativi, nella consapevolezza che la tempestiva rilevazione e correzione delle debolezze rappresenta una misura fondamentale di riduzione del rischio.

L'organizzazione si impegna a:

- Raccogliere informazioni sulle vulnerabilità tecniche attraverso scansioni periodiche dei dispositivi aziendali, avvisi dei fornitori e fonti pubbliche riconosciute, anche a seguito di cambiamenti significativi dell'infrastruttura.
- Valutare l'esposizione ai rischi connessi a ciascuna vulnerabilità rilevata, classificandone la gravità e attribuendo priorità di trattamento proporzionate all'impatto potenziale.
- Definire e attuare le azioni correttive — applicazione di patch, modifiche di configurazione o misure compensative — con tempistiche commisurate al livello di rischio, documentando ogni intervento nel relativo registro.
- Verificare l'efficacia delle azioni intraprese e mantenere aperto il monitoraggio fino alla conferma della risoluzione.

Gestione del cambiamento

Ogni modifica alle strutture di elaborazione delle informazioni e ai sistemi informativi — compresi aggiornamenti, sostituzioni di componenti, variazioni architetture e modifiche

delle configurazioni di rete — è sottoposta a un processo controllato di gestione del cambiamento. L'organizzazione richiede che ogni cambiamento sia:

- Descritto e motivato dal promotore, con indicazione dell'ambito di impatto.
- Valutato nei suoi effetti sulla sicurezza, sulla disponibilità dei servizi e sulla documentazione del sistema di gestione.
- Autorizzato prima dell'implementazione, sulla base di una valutazione dei rischi associati.
- Documentato formalmente attraverso il *MOD Gestione del cambiamento* , con registrazione dello stato di avanzamento e dell'esito della validazione.

Le modalità operative per la pianificazione, l'autorizzazione e il monitoraggio dei cambiamenti sono definite nella *PRO Procedura di gestione del cambiamento* .

Archiviazione e aggiornamento

La presente politica è conservata nel sistema documentale dell'organizzazione e resa accessibile a tutto il personale rientrante nel campo di applicazione, secondo le modalità definite dalla *PRO Procedura di gestione delle informazioni documentate* . Il **Responsabile del sistema di gestione** ne assicura il riesame almeno annuale e comunque in occasione di cambiamenti significativi del contesto organizzativo, tecnologico o normativo. Ogni revisione è soggetta ad approvazione della Direzione prima della diffusione.

Documenti di riferimento

- PRO Procedura di continuità operativa e di ripristino di emergenza
- POL Politica di protezione delle PII
- POL Politica di conservazione e cancellazione delle informazioni
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione della sicurezza della rete
- PRO Procedura di gestione del cambiamento
- PRO Procedura di gestione delle informazioni documentate
- MOD Gestione del cambiamento
- MOD Diagramma di rete
- MOD Modulo di assegnazione dei beni
- Registro degli utenti autorizzati all'uso delle informazioni

POL Politica di classificazione ed etichettatura delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	12/01/2026	Valerio patti	Antonino De Vita

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Classificazione delle informazioni
- Etichettatura delle informazioni
- Gestione delle informazioni
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

Tekna adotta la presente politica per istituire un quadro di riferimento unitario per la classificazione e l'etichettatura di tutte le informazioni e degli asset informativi aziendali. L'organizzazione riconosce che la protezione delle informazioni rappresenta un fattore abilitante della propria attività di ingegneria e consulenza tecnica nel settore delle telecomunicazioni, delle energie rinnovabili e delle infrastrutture, e si impegna a garantire che a ciascun asset informativo sia associato un livello di protezione adeguato al suo valore, alla sua sensibilità e al rischio correlato.

Attraverso questa politica l'organizzazione persegue i seguenti obiettivi:

- Definire un sistema di classificazione a tre livelli che rifletta le esigenze di riservatezza, integrità e disponibilità delle informazioni, nonché i requisiti legali e contrattuali applicabili.
- Stabilire regole di etichettatura che rendano immediatamente riconoscibile il livello di protezione associato a ogni informazione, indipendentemente dal formato o dal supporto.
- Assicurare che il trattamento, la trasmissione, la conservazione e lo smaltimento delle informazioni avvengano in coerenza con la classificazione assegnata, contribuendo alla prevenzione di accessi non autorizzati, fughe di dati e perdite informative.

Campo di applicazione

La presente politica si applica a tutte le informazioni gestite da Tekna — in formato digitale, cartaceo o su qualsiasi altro supporto — e a tutti i sistemi informativi che le elaborano o le conservano, presso la sede operativa di Via Armando Diaz 41, Marsala. Essa vincola tutto il personale dipendente, i collaboratori a partita IVA e le terze parti autorizzate ad accedere alle informazioni aziendali, inclusi i fornitori di servizi professionali con i quali sia in vigore un accordo di trattamento dati.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679

Termini e definizioni

- **Classificazione delle informazioni:** processo di categorizzazione delle informazioni in base alle esigenze di sicurezza dell'organizzazione relativamente alla riservatezza, all'integrità, alla disponibilità e ai requisiti delle parti interessate, al fine di assegnare un livello di protezione proporzionato.

- **Etichettatura delle informazioni:** apposizione di un contrassegno fisico o digitale che rende visibile il livello di classificazione attribuito a un'informazione, facilitandone il corretto trattamento da parte di chiunque ne entri in possesso.
- **Proprietario delle informazioni:** persona o funzione aziendale cui è attribuita la responsabilità primaria per la gestione, la protezione e la classificazione di uno specifico insieme di informazioni.
- **Supporto di memorizzazione:** qualsiasi dispositivo fisico o virtuale destinato a registrare, conservare o trasportare informazioni, inclusi dischi rigidi, unità USB, supporti ottici, servizi cloud e archivi cartacei.
- **Cancellazione sicura:** processo irreversibile che rende le informazioni irrecuperabili dal supporto su cui erano memorizzate, anche mediante tecniche forensi avanzate.

Ruoli e responsabilità

- **Responsabile del sistema di gestione:** supervisiona l'attuazione della presente politica, ne verifica il rispetto attraverso attività di audit e gestisce le eventuali richieste di eccezione o le segnalazioni di violazione.
- **Top Management:** approva la presente politica, autorizza i trasferimenti di informazioni riservate verso terzi e dispone eventuali sospensioni della cancellazione in caso di obblighi legali.
- **Proprietari delle informazioni:** classificano le informazioni sotto il proprio controllo, ne riesaminano periodicamente la classificazione, approvano le richieste di accesso e identificano requisiti di protezione aggiuntivi.
- **Tutto il personale e le terze parti autorizzate:** custodiscono le informazioni in conformità alla classificazione ed etichettatura assegnata, segnalano tempestivamente eventuali anomalie e rispettano le misure di protezione stabilite per ciascun livello.

Classificazione delle informazioni

Tekna classifica le proprie informazioni sulla base delle esigenze di riservatezza, integrità e disponibilità, dei requisiti legali e contrattuali e della criticità per il business. Il sistema di classificazione adottato dall'organizzazione si articola in tre livelli, ordinati dal più restrittivo al meno restrittivo. Ogni sistema informatico è classificato in base al livello più elevato delle informazioni che memorizza o elabora.

Riservato — Rientrano in questo livello le informazioni la cui divulgazione non autorizzata comporterebbe un danno grave per l'organizzazione, per i suoi clienti o per le persone fisiche coinvolte. L'accesso è strettamente limitato a ruoli specifici e pre-autorizzati.

Esempi: dati personali identificativi dei dipendenti e dei collaboratori, dati finanziari e bancari, informazioni sulle retribuzioni, credenziali di autenticazione e chiavi crittografiche, piani strategici aziendali, documentazione relativa ai rapporti con operatori di telecomunicazioni contenente clausole di riservatezza contrattuale.

Limitato — Comprende le informazioni proprietarie dell'organizzazione che, pur non raggiungendo il livello di sensibilità delle informazioni riservate, richiedono protezione per

preservare gli interessi aziendali. L'accesso è concesso esclusivamente al personale che ne ha una comprovata necessità operativa. Questo livello costituisce la classificazione predefinita per tutte le informazioni aziendali non diversamente classificate.

Esempi: procedure interne del sistema di gestione, contratti con clienti e fornitori, verbali di riunione, report interni sulle commesse, comunicazioni e-mail interne a contenuto operativo, registri del sistema di gestione.

Pubblico — Include le informazioni destinate alla diffusione esterna o il cui accesso da parte di soggetti terzi non comporta rischi per l'organizzazione.

Esempi: materiale di marketing, descrizioni dei servizi di ingegneria offerti, politiche del sistema di gestione comunicate agli stakeholder esterni, informazioni già rese pubbliche dall'organizzazione.

Etichettatura delle informazioni

L'etichettatura è il meccanismo attraverso cui la classificazione di un'informazione viene resa immediatamente visibile, così da garantire un trattamento coerente con il livello di protezione richiesto. Tekna si impegna ad applicare l'etichettatura a tutte le informazioni classificate come "Riservato" o "Limitato"; le informazioni pubbliche non richiedono un'etichetta specifica, poiché l'assenza di contrassegno denota il livello a minor restrizione.

Le modalità di etichettatura variano in funzione del supporto:

- **Documenti elettronici** — Ogni documento digitale classificato riporta l'etichetta corrispondente (ad esempio "RISERVATO" o "LIMITATO") nell'intestazione, nel piè di pagina o come filigrana, in modo che sia visibile sia a video sia in stampa.
- **Comunicazioni e-mail** — Le e-mail che veicolano informazioni classificate includono l'etichetta di classificazione nel campo oggetto, anteposta al titolo del messaggio.
- **Supporti fisici** — I documenti cartacei sono contrassegnati con l'etichetta in posizione ben visibile sulla prima pagina o sulla copertina. I supporti di memorizzazione rimovibili il cui utilizzo sia stato eccezionalmente autorizzato — quali unità USB o dischi esterni — riportano un'etichetta fisica che ne identifica la classificazione massima contenuta.

L'organizzazione promuove la coerenza tra classificazione ed etichettatura lungo l'intero ciclo di vita dell'informazione: qualora la classificazione venga modificata a seguito di riesame, l'etichettatura è aggiornata tempestivamente dal proprietario delle informazioni.

Gestione delle informazioni

Trattamento delle informazioni

Tekna adotta requisiti di protezione differenziati in funzione del livello di classificazione, al fine di assicurare che ogni informazione sia trattata in modo proporzionato al rischio connesso alla sua compromissione.

Informazioni Riservate — L'organizzazione sottopone queste informazioni ai controlli più rigorosi. L'accesso è concesso soltanto a ruoli espressamente autorizzati, tracciato mediante il *Registro degli utenti autorizzati all'uso delle informazioni* e fondato sul principio

del minimo privilegio. I sistemi che le ospitano non ammettono accessi anonimi e richiedono l'autenticazione a due fattori. Le informazioni riservate sono crittografate sia in fase di archiviazione (at-rest) — mediante algoritmi conformi alle pratiche stabilite nella *PRO Procedura di crittografia e gestione delle chiavi crittografiche* — sia durante la trasmissione su reti pubbliche (in-transit). I dispositivi mobili e i laptop che le contengono dispongono di cifratura completa del disco e di blocco schermo automatico dopo un breve periodo di inattività, protetti da password o biometria. I backup di queste informazioni sono parimenti crittografati. L'archiviazione su dispositivi personali o supporti rimovibili non approvati è vietata, così come l'invio verso servizi cloud non autorizzati dall'organizzazione.

Informazioni Limitate — L'accesso è concesso esclusivamente sulla base di una comprovata necessità operativa (need-to-know). I sistemi che le ospitano non consentono accessi anonimi e richiedono credenziali personali conformi alla politica aziendale sulle password. I documenti cartacei classificati come Limitato sono conservati in ambienti ad accesso controllato e smaltiti in modo sicuro al termine del ciclo di vita. Copie non autorizzate non sono ammesse.

Informazioni Pubbliche — Non richiedono controlli di accesso specifici e possono essere distribuite liberamente all'esterno, purché la loro diffusione sia stata preventivamente autorizzata dal proprietario delle informazioni.

L'organizzazione si impegna altresì ad applicare misure di prevenzione della fuga di dati su tutti i sistemi, le reti e i dispositivi che elaborano, archiviano o trasmettono informazioni classificate come Riservato o Limitato. Tali misure comprendono il controllo degli endpoint attraverso soluzioni di sicurezza in grado di bloccare trasferimenti non autorizzati, il monitoraggio delle attività di rete e la restrizione dell'utilizzo di supporti rimovibili e servizi di condivisione non approvati.

Trasferimento delle informazioni

Tekna disciplina il trasferimento delle informazioni verso soggetti esterni con regole proporzionate alla classificazione, perseguendo l'obiettivo di prevenire la divulgazione non autorizzata e di garantire la tracciabilità di ogni scambio significativo.

Il trasferimento a terzi di informazioni **Riservate** è consentito unicamente in presenza di un vincolo legale o contrattuale che ne legittimi la comunicazione e con l'esplicita autorizzazione del **Top Management** o del proprietario delle informazioni. Prima del trasferimento deve essere verificata l'esistenza di un accordo di riservatezza o di clausole contrattuali equivalenti.

Analogamente, il trasferimento di informazioni **Limitate** richiede l'approvazione del **Top Management** e un accordo di confidenzialità con il destinatario. Tutti i trasferimenti elettronici di informazioni Riservate o Limitate avvengono attraverso canali cifrati — PEC con crittografia TLS, SFTP o portali clienti protetti — e sono documentati con l'indicazione di data, mittente, destinatario, canale utilizzato, tipologia di informazione e misure di sicurezza applicate.

Il trasferimento di informazioni mediante supporti fisici rimovibili — unità USB, dischi esterni o plichi cartacei — è tracciato in un apposito registro che riporta l'identificativo del supporto, il mittente, il destinatario, la data e l'ora di uscita e l'eventuale cifratura applicata. L'uso di supporti rimovibili non cifrati per informazioni Riservate è vietato.

Le informazioni **Pubbliche** possono essere trasferite senza restrizioni particolari, nel rispetto della coerenza con la comunicazione istituzionale dell'organizzazione.

Supporti di memorizzazione

L'organizzazione gestisce i supporti di memorizzazione lungo l'intero ciclo di vita — acquisizione, utilizzo, trasporto e smaltimento — in conformità con la classificazione delle informazioni in essi contenute. Tekna promuove l'utilizzo dei sistemi cloud aziendali approvati come canale primario di archiviazione e limita l'impiego di supporti rimovibili ai soli casi in cui l'operatività lo renda strettamente necessario e previa autorizzazione del **Responsabile del sistema di gestione**.

I supporti che contengono informazioni Riservate o Limitate sono conservati in ambienti ad accesso controllato e non possono essere lasciati incustoditi in luoghi pubblici o comuni. Il trasporto avviene sotto la custodia diretta del personale autorizzato, e il prestito o il trasferimento a terzi è subordinato al rispetto delle regole di trasferimento stabilite dalla presente politica. La *PRO Procedura di configurazione, gestione e smaltimento degli asset* dettaglia i criteri operativi per la classificazione, la manutenzione e la tracciabilità degli asset fisici.

Smaltimento sicuro e riutilizzo delle apparecchiature

Tekna si impegna a garantire che nessuna informazione classificata possa essere recuperata da apparecchiature o supporti dismessi o riassegnati. Prima dello smaltimento o del riutilizzo, ogni supporto di memorizzazione è sottoposto a operazioni di cancellazione sicura con tecniche adeguate alla tipologia del media:

- Sovrascrittura multipla per supporti magnetici.
- Cancellazione crittografica (distruzione della chiave di cifratura) per supporti SSD e storage cifrato.
- Degaussing o distruzione fisica per supporti che non ammettono cancellazione logica verificabile.

I materiali cartacei contenenti informazioni Riservate o Limitate sono distrutti mediante distruggi-documenti prima dello smaltimento. Ogni operazione di sanitizzazione è registrata con indicazione della data, dell'identificativo del supporto, della tecnica utilizzata, dell'esito e del responsabile. Lo smaltimento finale delle apparecchiature dismesse avviene attraverso fornitori qualificati per la gestione dei rifiuti elettronici, nel rispetto della normativa ambientale applicabile.

Cancellazione delle informazioni

L'organizzazione riconosce che la conservazione di informazioni oltre il termine di necessità operativa, legale o contrattuale incrementa l'esposizione al rischio e viola il principio di minimizzazione dei dati. Tekna adotta periodi di conservazione definiti per ciascuna categoria di informazioni, documentati nel *MOD Conservazione delle informazioni e degli asset*, e ne riesamina l'adeguatezza con cadenza almeno annuale.

Al termine del periodo di conservazione stabilito, le informazioni sono cancellate in modo sicuro e irreversibile secondo le tecniche indicate nella sezione precedente. File temporanei generati durante il normale funzionamento dei sistemi sono individuati e rimossi entro un periodo definito quando non più necessari. In presenza di obblighi di conservazione derivanti da procedimenti giudiziari, indagini o audit, il **Top Management** dispone la sospensione della cancellazione (legal hold) fino alla cessazione del vincolo, informandone il **Responsabile del sistema di gestione**. La *POL Politica di conservazione e cancellazione delle informazioni* disciplina nel dettaglio le responsabilità e le modalità operative del ciclo di vita dei dati.

Protezione delle informazioni di test

Tekna si impegna a proteggere le informazioni utilizzate a supporto delle attività di test — validazione di configurazioni, verifiche di accettazione e controllo qualità — con il medesimo rigore riservato ai dati di produzione, quando la loro natura lo richieda. I dataset di test sono selezionati in modo da evitare l'esposizione di dati reali sensibili o personali; qualora l'uso di dati reali risulti indispensabile, si applicano tecniche di anonimizzazione, pseudonimizzazione o mascheramento prima dell'impiego. A ogni dataset è attribuita una classificazione coerente con il contenuto effettivo, e le misure di protezione corrispondono a quelle previste per il livello assegnato. La conservazione dei dataset di test è limitata al tempo strettamente necessario, al termine del quale si procede alla cancellazione sicura.

Archiviazione e aggiornamento

La presente politica è un documento controllato del Sistema di Gestione della Sicurezza delle Informazioni e viene conservata in formato digitale all'interno della piattaforma documentale aziendale, accessibile al personale autorizzato in conformità con la propria classificazione. Il **Responsabile del sistema di gestione** ne cura il riesame con cadenza annuale, oppure a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia, nel contesto normativo o nel panorama delle minacce. Ogni modifica approvata dal **Top Management** comporta l'aggiornamento dell'indice di revisione e la comunicazione a tutto il personale interessato, secondo le modalità definite nella *PRO Procedura di gestione delle informazioni documentate*.

Documenti di riferimento

- PRO Procedura di gestione delle informazioni documentate
- POL Politica di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di conservazione e cancellazione delle informazioni
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di crittografia e gestione delle chiavi crittografiche