ACCEPTABLE USE POLICY

INFORMAZIONI SUL DOCUMENTO

Registro delle modifiche

Rev.	Data	Descrizione	Stato	Redazione	Verifica	Approvazione
3.8	12/01/2023	Inserimento dei riferimenti ai servizi fiduciari e ristrutturazione del documento	Approvato	Michele Paradiso	Stefano Liguori	Fulvio Talucci
3.9	17/07/2023	Revisione e aggiornamento delle informazioni	Approvato	Michele Paradiso	Stefano Liguori	Fulvio Talucci
4.0	19/02/2024	Revisione delle informazioni	Approvato	Catello Cascone	Michele Paradiso	Stefano Liguori
4.1	06/11/2024	Richiamo alla Policy per l'utilizzo risorse informatiche	Approvato	Catello Cascone	Michele Paradiso	Stefano Liguori
5.0	19/03/2026	Aggiornato registro modifiche. Aggiornato il riferimento della ISO/IEC 27018.	Approvato	IT Risk & Compliance	IT Risk & Compliance Manager	CIO

Classificazione

- Livello di Classificazione: USO INTERNO
- Documentazione disponibile nello SharePoint Aziendale all'area ISO - Sistema di Gestione della Sicurezza delle Informazioni
- Accesso Limitato al personale indicato nella Lista degli Accessi di seguito riportata

Lista degli Accessi

No.	Role	Sola Lettura	Lettura e Modifica
1	Direzione Aziendale		X
2	Responsabile Sicurezza Informatica		X
3	Tutto il personale	X	

Altre informazioni sul documento

- N° Allegati: 0

SOMMARIO

1. INTRODUZIONE

Le Risorse Informatiche fornite da TeamSystem ai propri dipendenti (postazioni di lavoro fisse e mobili, posta elettronica, Internet) supportano lo svolgimento del lavoro e dei compiti dei dipendenti.
Le informazioni in essi contenute sono da considerarsi come patrimonio aziendale e, in linea con quanto previsto dalla normativa sulla privacy (rif.[4],[5]), come tale devono essere tutelate.

1.1 Scopo

Obiettivo del presente documento è tradurre gli obiettivi ed i requisiti di sicurezza espressi nell'Information Security Policy (rif.[1]) in misure di sicurezza che il personale di TeamSystem è tenuto ad adottare nello svolgimento delle proprie mansioni, al fine di garantire l'utilizzo corretto e sicuro degli strumenti informatici e la protezione dell'intero patrimonio informatico gestito.
Per tutto ciò che non è contemplato nel presente documento, si faccia riferimento alla "Policy *per utilizzo risorse informatiche".*

1.2 Campo di Applicazione

TeamSystem, in qualità di depositario di un ampio volume di informazioni rilevanti, si assume la piena responsabilità per quanto attiene il trattamento e la protezione dei dati custoditi. Tale responsabilità deve essere attribuita, con diversi gradi e in differente modalità (a seconda delle proprie competenze, dei compiti assegnati e delle operazioni eseguite), a tutti coloro che hanno accesso alle informazioni; sono quindi compresi i Dipendenti, ma anche le Terze Parti.
Sono oggetto di questa politica tutti i sistemi informativi e le infrastrutture dedicate all'erogazione dei servizi ai Clienti finali di tutti i servizi di TeamSystem.

2. DEFINIZIONI E RIFERIMENTI

Le seguenti definizioni sono in linea con quanto indicato all'interno dello standard ISO/IEC 27000 (rif. [3])

Disponibilità
Proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.

Incaricato al trattamento
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento. È tenuta a fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Integrità
Proprietà relativa alla salvaguardia dell'accuratezza e della completezza dei beni.

Internet
Una rete logica complessa, appoggiata a strutture fisiche e collegamenti di vario tipo (fibre ottiche, collegamenti satellitari, doppino telefonico, ponti radio) che interconnette persone o dispositivi automatici tramite qualsiasi tipo di computer o elaboratore elettronico.

Need to know
Principio per cui l''utente accede soltanto ai dati strettamente necessari per eseguire le attività di propria competenza (i.e. secondo le mansioni assegnate aziendalmente).

Posta elettronica
Modalità di scambio di messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente.

Riservatezza
Proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati.

Segregation of Duty
Principio che mira a separare le attività in modo da evitare la concentrazione di più attività critiche nelle mani della stessa persona / funzione.

SGSI (Sistema di Gestione per la Sicurezza delle Informazioni) o ISMS (Information Security Management System)
Insieme delle politiche, procedure, linee guida, risorse e attività associate, gestite da un'organizzazione al fine di proteggere i propri asset informativi. Un SGSI è un approccio sistematico per stabilire, attuare, condurre, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni di un'organizzazione per raggiungere gli obiettivi di business.

Sicurezza delle informazioni
Conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni; inoltre, possono essere coinvolte altre proprietà quali l'autenticità, la responsabilità, il non ripudio e l'affidabilità.

Spam
L'insieme dei messaggi di posta inviati senza il permesso del destinatario, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, da discutibili progetti finanziari a veri e propri tentativi di truffa

Titolare del trattamento
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Riferimenti

[1] PO_SEC_00_Information Security Policy
[2] ANNEX A – Gestione sicura della documentazione
[3] ISO/IEC 27000:2018 - Information Technology — Security Techniques — Information Security Management Systems — overview and vocabulary
[4] D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali, così come modificato dal D.Lgs 101/2018 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).*"
[5] Regolamento UE n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati)
[6] Legge 20 maggio 1970, n. 300 (art. 4 impianti audiovisivi);
[7] IT_PAW_00_Procedura assegnazione dispositivi fissi e mobili
[8] ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
[9] ISO/IEC 27018:2025 Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors
[10] ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
[11] PO_GA_00SPQ_Politica_Gestione Accessi_Servizi IDP SPID_QTSP
[12] PR_BKP_00_Salvataggio e Ripristino dei dati
[13] PR_LOG_00_Procedura Log Management
[14] PR_GSU_00_Gestione accessi logici
[15] ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls

3. PRINCIPI GENERALI DELLA SICUREZZA DELLE INFORMAZIONI

I danneggiamenti ai sistemi informatici (intenzionali o meno) sono agevolati da comportamenti negligenti dell'utente che, in assenza di un controllo preventivo e di prescrizioni puntuali, potrebbe installare programmi nocivi al sistema, scaricare allegati sospetti disattivando la protezione, comunicare password, essere vittima di un attacco informatico.
Al fine di garantire la sicurezza del patrimonio informativo aziendale, il Gruppo ha definito delle regole comportamentali da adottare per l'utilizzo consono e consapevole delle informazioni e degli strumenti aziendali ad essi connessi, relative ai seguenti ambiti:

- utilizzo delle risorse informatiche aziendali;
    - clear desk e clear screen policy;
    - utilizzo della posta elettronica come strumento lavorativo;
    - impiego di internet come strumento lavorativo;
    - utilizzo della postazione di lavoro;
    - utilizzo di supporti fisici removibili;
- gestione degli accessi logici e degli accessi da remoto;
- backup e restore

3.1 Utilizzo delle risorse informatiche aziendali

Di seguito sono riportate le norme comportamentali per il corretto utilizzo di tutte le risorse aziendali che il Gruppo mette a disposizione degli utenti:

- Clear desk e clear screen policy:
    - Non lasciare documenti contenenti informazioni e dati privati, sensibili, critici, ecc. sulla propria scrivania e sullo schermo del proprio computer;
    - L'utente non deve memorizzare sulla Postazione di Lavoro archivi di qualsiasi genere relativi ai clienti o comunque collegati ai servizi a questi ultimi erogati;
    - Prima di allontanarsi per brevi periodi dalla propria postazione di lavoro, il contenuto di eventuali informazioni non pubbliche in evidenza sulla scrivania deve essere celato dagli sguardi di eventuali persone non autorizzate e la postazione deve essere bloccata;
    - Nel caso di assenza prolungata e comunque al termine della normale attività lavorativa giornaliera occorre rimuovere dalla propria scrivania tutte le informazioni non pubbliche riponendole in luoghi idonei al tipo di classificazione (es. armadi o cassettiere con serratura).
- Utilizzo della posta elettronica come strumento lavorativo:
    - Per tutelare la riservatezza delle informazioni è necessario che queste siano divulgate e distribuite solo alle persone che abbiano effettivamente il diritto di conoscerle (principio del "need to know");
    - Nella trasmissione di messaggi di posta elettronica sia verso l'esterno che verso l'interno del Gruppo, l'utente è tenuto ad osservare i criteri di sicurezza per la classificazione delle informazioni;
    - Lo scambio di informazioni classificate "Confidenziali" verso rete esterna deve essere effettuato utilizzando adeguate tecniche di cifratura dei dati. Ove non siano disponibili specifici strumenti in tal senso è consentito l'invio di file compressi con password, purché la password sia comunicata tramite l'invio di un'ulteriore mail;

- Per non appesantire la rete aziendale sono vietate le attività di inoltro massivo di comunicazioni, salvo che non siano preventivamente autorizzate per l'invio di messaggi a tutti i dipendenti;
- È vietato spedire mail che, per forma o contenuto, possano ledere l'immagine del Gruppo o compromettere le relazioni con clienti, fornitori o Terzi;
- È vietato spedire mail che possano risultare diffamatorie, oscene od offensive tali da recare danno o che possano essere considerate da altri fonte di discriminazione religiosa, razziale, sessuale, politica, sindacale;
- È vietato spedire mail indesiderate a fini commerciali non attinenti all'attività lavorativa (Spamming);
- Non è consentito spedire messaggi di carattere personale.

- Impiego di internet come strumento lavorativo:
  - L'accesso a Internet è messo a disposizione degli utenti per lo svolgimento delle proprie mansioni lavorative ovvero per il reperimento di informazioni utili a tale scopo;
  - Gli utenti collegati a Internet devono essere consapevoli che l'utilizzo improprio di questo servizio può avere conseguenze in termini di etica, di immagine e di sicurezza per il Gruppo;
  - Non è consentita la navigazione su siti considerati di natura "sconveniente", intendendo tutti i siti web il cui contenuto sia non solo inconsistente con le normali attività professionali e con gli incarichi che il dipendente è chiamato a svolgere, ma contrario alle comuni norme etiche e morali.
- Utilizzo delle postazioni di lavoro (fissa o mobile) in dotazione agli utenti:
  - L'utente non deve modificare la configurazione hardware e software della Postazione di Lavoro rispetto allo standard definito e fornito dal Gruppo;
  - Non è consentito l'installazione di software senza esplicita autorizzazione del Dipartimento IT;
  - L'utente deve sempre attivare la password di accesso alla propria Postazione di Lavoro, e bloccarla ogni volta che questa è lasciata incustodita anche per brevi periodi;
  - Nel caso in cui la Postazione di Lavoro portatile venga portata all'esterno dell'organizzazione, l'utente deve proteggere il computer da eventuali furti, danneggiamenti o smarrimenti;
  - L'utente non deve interferire, impedire o ritardare gli aggiornamenti del software della postazione di lavoro quando questo avviene in maniera centralizzata e deve procedere all'aggiornamento manuale del software installando quanto indicato dal Dipartimento IT;
  - È vietato riprodurre copie del software aziendale protetto da licenza di utilizzo o da norme a tutela dei diritti d'autore;
  - L'utente deve verificare che il programma di antivirus installato e mantenuto centralmente dall'azienda sulla Postazione di Lavoro sia sempre attivo e costantemente aggiornato;
  - L'utente non deve aprire le mail di provenienza sconosciuta e/o con contenuto sospetto ma avvisare prontamente l'Amministratore di sistema perché possa provvedere alle opportune verifiche di sicurezza; inoltre non deve eseguire programmi ricevuti come allegati a messaggi di posta elettronica o ottenuti mediante download da siti web senza preventivamente averli scaricati sulla Postazione di Lavoro ed averli sottoposti a controllo con antivirus;
  - Qualora si verifichi un'infezione da virus informatico l'utente è tenuto a comunicare l'accaduto al Responsabile della sicurezza informatica secondo le modalità definite in [1] che provvederà a prendere le cautele del caso.

Nello specifico, l'utilizzo di postazioni mobili al di fuori del perimetro aziendale prevede una particolare attenzione nell'applicazione delle seguenti misure di sicurezza:

- Bloccare lo schermo quando ci si allontana;
- Fare attenzione durante l'inserimento di credenziali;
- Proteggere gli strumenti di lavoro da incidenti domestici;
- Ricordare di cambiare periodicamente la password in caso di tethering.

Per ulteriori approfondimenti si rimanda al documento (rif.[7]).

- Utilizzo di supporti fisici removibili:
  - L'utilizzo dei supporti fisici removibili (es. chiavi USB, memorie SD, hard disk esterno, altro), è autorizzato solo a scopo professionale ma esclusivamente per attività non correlate con l'erogazione dei servizi ai Clienti, quali ad esempio il servizio di Fatturazione Elettronica o di Conservazione Cloud. Il loro utilizzo è consentito ad esempio per:
    - lo scambio di informazioni tra due dipendenti qualora essi si trovino al di fuori dei locali TeamSystem o in assenza di collegamenti di rete;
    - lo scambio di file di notevoli dimensioni, al fine di non saturare o degradare il livello di performance della rete.
  - I dati devono essere copiati applicando algoritmi crittografici standard (e.g., AES256);
  - L'utilizzo di questi strumenti deve essere limitato al periodo strettamente necessario ed i dati memorizzati devono essere rimossi non appena cessi l'esigenza che ha determinato l'utilizzo della memoria di massa removibile;
  - Nel caso in cui la memoria di massa sia utilizzata per trasferire i dati ad un Terzo (i.e. Clienti e/o altri professionisti) è preferibile utilizzare chiavi fornite da detti Terzi. Nel caso in cui ciò non sia possibile è necessario utilizzare una memoria di massa precedentemente formattata;
  - Gli Utenti non sono autorizzati a trattenere memorie di massa fornite da Terzi. Nel caso in cui la memoria di massa sia utilizzata per trasferire dati ad un collega, l'Utente è tenuto a copiare esclusivamente i file a fini professionali e limitatamente all'attività in corso. I dati devono essere cancellati dalla memoria di massa immediatamente dopo la copia e/o l'utilizzo;
  - È necessario che sul supporto non siano apposti riferimenti all'ente produttore o ai dati/metadati contenuti all'interno del supporto.

3.2 Dismissione degli asset aziendali

La fase di dismissione degli asset dell'organizzazione rappresenta una delle fasi più critiche sotto il profilo sicurezza delle informazioni; la non corretta adozione delle direttive e delle procedure stabilite dalla Direzione Aziendale potrebbero compromette la salvaguardia del patrimonio informativo aziendale e il conseguente aumento dei rischi connessi.

L'Organizzazione si avvale di appositi strumenti organizzativi ed informatici per gestire la dismissione sicura degli asset (e.g. PC, notebook, supporti di memorizzazione esterni) e salvaguardare la riservatezza delle informazioni in essi contenuti, onde evitare che alcun tipo di informazione o di software possa accidentalmente entrare in possesso di soggetti non autorizzati.

Ogni asset restituito al personale tecnico dai dipendenti, ad esempio nel caso di dimissionari, prevede la compilazione di un apposito modulo firmato dalle figure responsabili e dal dipendente. Contestualmente, il personale tecnico competente provvede alla cancellazione sicura dei dati elettronici salvati all'interno del dispositivo (secure wiping) mediante utilizzo di software dedicato.

Lo strumento adottato per la cancellazione sicura è Eraser (http://eraser.heidi.ie/), installato su tutte le workstation e su tutti i server coinvolti nell'erogazione dei servizi che trattano informazioni confidenziali o di proprietà dei clienti di TeamSystem Service (e.g., Fatturazione Elettronica alla PA, Conservazione Cloud), considerando sia l'ambiente di produzione, sia di sviluppo e collaudo.

I supporti rimovibili, terminata la loro funzione, dovranno essere cancellati o preferibilmente eliminati in maniera sicura tramite gli strumenti messi a disposizione dal Dipartimento IT di Gruppo.

Lo smaltimento sicuro degli archivi cartacei è invece garantito tramite l'utilizzo di appositi strumenti per la distruzione dei documenti cartacei disponibili presso tutte le sedi delle società del Gruppo TeamSystem.

3.3 Gestione degli accessi logici

L'accesso alle risorse informatiche e di rete ed i privilegi associati a tali accessi sono limitati a quelli indispensabili per le proprie esigenze lavorative. L'accesso alle risorse informatiche deve avvenire mediante account nominali. Non è consentito l'accesso ai sistemi mediante utenze di gruppo.
Le utenze non utilizzate per un periodo di tre mesi vengono sospese temporaneamente, previa notifica all'interessato. Ove non pervenissero comunicazioni formali di riabilitazione dello stesso nei successivi due mesi, l'account in questione viene "cessato".
Gli utenti e gli operatori devono essere informati circa la responsabilità relativa all'utilizzo ed alla custodia delle credenziali, password.
Ulteriori dettagli relativi alla procedura degli accessi logici sono descritti nella procedura.

3.4 Backup

È compito dell'utente eseguire periodicamente delle attività di backup per la conservazione delle informazioni contenute nelle proprie Postazione di Lavoro.

4. CONTROLLO AZIENDALE A TUTELA E SALVAGUARDIA DEL PATRIMONIO AZIENDALE

L'abuso degli strumenti informatici affidati da TeamSystem ai propri dipendenti per lo svolgimento delle mansioni, espone al rischio della commissione di illeciti nonché di un coinvolgimento del Gruppo stesso in responsabilità di natura sia civile sia penale.

Nasce l'esigenza da parte di TeamSystem di tutelarsi preventivamente con l'adozione delle opportune misure per evitare la commissione di illeciti da parte del dipendente, nonché per tentare di fornire la prova di aver fatto il possibile per evitare l'illecito, ed essere conseguentemente sollevata da responsabilità.

TeamSystem può trovarsi nella condizione di dover avere accesso ai log di navigazione relativi all'accesso Internet per poter risalire all'utente che ha effettuato (o ha tentato di effettuare) una determinata operazione.

Tipicamente i file di log sono resi disponibili per:

- l'analisi delle segnalazioni di errore;
- la produzione di statistiche di esercizio, come ad esempio quelle del traffico nei servizi web;
- il ripristino di situazioni precedenti;
- l'analisi delle modifiche alle basi dati;
- l'analisi delle operazioni eseguite e dei responsabili di tali operazioni;
- la ricostruzione degli eventi;
- l'attribuzione delle responsabilità;
- l'analisi e comprensione all'interno del Gruppo su chi utilizza i sistemi e sul tipo di utilizzo effettuato;

- la conformità a leggi, norme e standard.

In linea con le best practice e gli standard internazionali e indipendentemente dalle sorgenti di log, il Gruppo ha individuato diverse tipologie di log in cui suddividere la vasta fonte di informazione legata al tracciamento:

- log di sistema - tracciano eventi di funzionamento di sistemi relativi a server, apparati di rete e dispositivi di sicurezza;
- log applicativi - tracciano eventi di funzionamento del software applicativo, utili sia per finalità di assistenza tecnica che ai fini di sicurezza;
- log di sicurezza - tracciano l'attività degli utenti, amministratori e non, relativamente alle diverse operazioni effettuate sui sistemi, sulle applicazioni e sui dati (log di accesso, comandi, cambi di configurazione, operazioni effettuate, ecc.);
- log di servizi - tracciano le attività svolte dai clienti che usufruiscono dei servizi messi a disposizione dall'Azienda.

Le attività di controllo e verifica dei log sono in capo al Gruppo che, è tenuto al rispetto delle seguenti regole:

- rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970) (rif.[6]);
- rispettare i principi di pertinenza e di non eccedenza, trattando solo i dati strettamente necessari per il raggiungimento delle finalità perseguite;
- designare per iscritto ad "Incaricato del trattamento" (art. 30 del Codice privacy [4], art. 29 del GDPR [5]) i soggetti preposti a detti trattamenti, impartendo loro adeguate istruzioni nel rispetto dei principi di necessità, pertinenza, liceità e correttezza;
- avere cura che i soggetti preposti accedano ai soli dati strettamente necessari per le finalità sopra riportate, evitando l'accesso a dati personali presenti in cartelle o spazi di memoria eventualmente assegnati a dipendenti/collaboratori;
- attenersi alle istruzioni sul tipo di controlli ammessi e sulle relative modalità di esecuzione descritte nel presente Regolamento;
- assicurarsi che venga svolta per i soggetti preposti un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

Per tutti i soggetti preposti ad attività di controllo sussiste l'obbligo di svolgere solo operazioni strettamente necessarie al perseguimento delle finalità indicate, senza realizzare attività di controllo di propria iniziativa.

5. VIOLAZIONE POLICY

La sicurezza delle informazioni riveste un ruolo essenziale nell'ottica dell'operatività aziendale ed è ottenuta definendo e implementando le politiche e le procedure definite all'interno della politica di sicurezza (rif.[1]). Pertanto, la violazione della stessa comporta la mancanza di adeguati livelli di sicurezza che può generare effetti negativi per l'Azienda, anche in termini di sanzioni legate alla violazione delle normative vigenti.

La Direzione si riserva di valutare eventuali provvedimenti disciplinari da intraprendere a seguito della violazione di tale policy.

PRESA VISIONE E ACCETTAZIONE

Il sottoscritto nato a il , dichiara di aver preso visione della *Acceptable Use Policy* e di accettarne i contenuti impegnandosi a rispettare i principi e i requisiti in essa definiti al fine di proteggere e tutelare il patrimonio informativo aziendale.

Luogo e data

_____

Dipendente