1. PREMESSA E CAMPO DI APPLICAZIONE

UNITIVA S.r.l., con sede a Napoli, opera da oltre quindici anni nell'**analisi, progettazione e sviluppo di soluzioni software e cloud management**, a supporto di aziende, enti e organizzazioni in molteplici settori (banking, energy, manufacturing, life science & healthcare, pubblica amministrazione), facendo leva su tecnologie open source e partner qualificati.

La presente **Politica della Sicurezza dei Dati** (di seguito "Politica") definisce principi, impegni e obiettivi che guidano l'implementazione e il miglioramento continuo del **Sistema di Gestione della Sicurezza dei Dati (SGSD)** conforme alla norma **ISO/IEC 27001:2022** (e relativo Emendamento 1:2024).

La Politica si applica a:

- tutte le informazioni trattate da UNITIVA, su qualsiasi supporto (digitale o cartaceo);
- tutti i processi rientranti nel campo di applicazione del SGSD:
  "Analisi, progettazione e sviluppo di soluzioni software e cloud management";
- tutto il personale di UNITIVA, a qualsiasi titolo operante (dipendenti, collaboratori, consulenti);
- tutti i soggetti esterni (fornitori, partner, outsourcer) che, a qualsiasi titolo, accedono a informazioni o sistemi ricompresi nel perimetro del SGSD.

L'osservanza della presente Politica è **obbligatoria** e deve essere recepita in contratti, accordi e procedure interne ed esterne pertinenti.

---

2. SCOPO E OBIETTIVI

Scopo della Politica è garantire che tutte le informazioni trattate da UNITIVA siano protette da minacce **interne ed esterne, intenzionali o accidentali**, in coerenza con i requisiti della ISO/IEC 27001:2022, delle normative cogenti (in particolare Reg. UE 2016/679 "GDPR") e degli impegni contrattuali assunti verso clienti e partner.
In particolare, UNITIVA persegue i seguenti **obiettivi generali**:

- assicurare la **riservatezza** delle informazioni, consentendone l'accesso solo a soggetti autorizzati;
- garantire l'**integrità** delle informazioni, preservandone accuratezza, completezza e affidabilità;
- garantire la **disponibilità** delle informazioni e dei servizi IT nei tempi e modi richiesti dal business e dagli accordi contrattuali;
- assicurare la **tracciabilità e la responsabilizzazione** (accountability) nel trattamento delle informazioni;
- prevenire e ridurre i rischi di violazioni di dati, incidenti di sicurezza, interruzioni di servizio, danni economici e reputazionali;

- tenere conto anche dei rischi e delle opportunità connessi ad eventi ambientali e al cambiamento climatico, laddove possano impattare la disponibilità e la sicurezza delle infrastrutture informatiche e fisiche;
- garantire la conformità a leggi, regolamenti, standard e impegni contrattuali applicabili (inclusi quelli in materia di protezione dei dati personali e sicurezza ICT);
- promuovere la **cultura della sicurezza** tra tutto il personale, attraverso formazione, consapevolezza e comportamenti coerenti.

Gli obiettivi specifici di sicurezza dei dati sono definiti, misurati e riesaminati secondo quanto previsto dal SGSD e dalla procedura di definizione degli obiettivi e dei riesami.

---

3. Principi di gestione della sicurezza dei dati

UNITIVA gestisce la sicurezza dei dati secondo i seguenti **principi generali**:

1. **Approccio basato sul rischio**: i rischi relativi alla sicurezza delle informazioni sono identificati, valutati e trattati in modo sistematico, utilizzando criteri documentati di accettazione del rischio, in conformità alle procedure di valutazione e trattamento dei rischi.
2. **Catalogo e classificazione degli asset**: esiste e viene mantenuto un **catalogo degli asset informativi e infrastrutturali**, con identificazione dei relativi proprietari e classificazione delle informazioni in base alla criticità (riservatezza, integrità, disponibilità).
3. **Controllo degli accessi**: l'accesso ai sistemi e alle informazioni avviene tramite processi di identificazione e autenticazione robusti, diritti di accesso basati su ruoli (principio del "need to know" e "least privilege") e riesami periodici delle autorizzazioni.
4. **Segregazione dei compiti e tracciabilità**: i compiti critici sono segregati quando necessario e le attività rilevanti sono tracciate tramite log e registrazioni protette.
5. **Integrazione nei processi**: i requisiti di sicurezza delle informazioni sono integrati in tutti i processi aziendali, inclusi progettazione, sviluppo, gestione delle infrastrutture, erogazione dei servizi, gestione dei fornitori e gestione delle modifiche.
6. **Miglioramento continuo**: il SGSD è oggetto di monitoraggio, audit interni, gestione di non conformità e azioni correttive, con l'obiettivo di migliorare continuativamente le prestazioni in materia di sicurezza dei dati.

---

4. Connessioni con terze parti, outsourcing e gestione dei fornitori

UNITIVA riconosce che le **connessioni con terze parti**, i servizi in outsourcing e i rapporti con fornitori e partner possono costituire un elemento critico per la sicurezza delle informazioni.

Per questo si impegna a:

- valutare i rischi relativi a fornitori, outsourcer, partner tecnologici e di connettività, inclusi data center, provider cloud, servizi di posta elettronica e repository;
- stipulare contratti e accordi che includano requisiti di sicurezza, riservatezza, protezione dei dati personali, livelli di servizio, gestione incidenti e obblighi di notifica;
- regolamentare e controllare le **connessioni di rete** e gli accessi remoti da parte di terze parti (VPN, accessi amministrativi, manutentori, partner applicativi), limitandoli al minimo necessario e monitorandone l'utilizzo;
- assicurare che le terze parti che trattano dati per conto di UNITIVA adottino misure di sicurezza almeno equivalenti a quelle previste dal SGSD;
- prevedere, ove necessario, specifiche valutazioni di impatto e misure aggiuntive per la gestione di dati particolarmente critici o sensibili (es. dati personali dei clienti finali dei nostri clienti).

---

5. GESTIONE DEI DATI E DEI RECORD (REGISTRAZIONI)

UNITIVA garantisce che i **record e le registrazioni** relativi alla sicurezza dei dati (log, audit trail, registrazioni di configurazione, documenti contrattuali, documenti di progetto, evidenze di audit, registri privacy, ecc.) siano:

- **accurati, completi e leggibili**;
- **identificabili e rintracciabili** rispetto all'attività, al sistema o al servizio cui si riferiscono;
- conservati per periodi coerenti con le norme di legge, gli obblighi contrattuali, le esigenze di business e le policy interne;
- adeguatamente protetti contro accessi non autorizzati, modifiche indebite, perdita o distruzione accidentale;
- soggetti a verifiche periodiche di qualità, aggiornamento e necessità di conservazione (valutazione dei record), con definizione di regole per l'archiviazione, l'aggiornamento e la cancellazione sicura.

---

6. PROTEZIONE DEI DATI PERSONALI, DATA MASKING E DIRITTO ALL'OBLIO

In coerenza con il GDPR e con il proprio sistema privacy, UNITIVA:

- applica il principio di **minimizzazione** dei dati personali trattati nel contesto dei servizi erogati;
- adotta tecniche di **pseudonimizzazione e data masking** per ridurre l'esposizione di dati personali e/o sensibili nei contesti di sviluppo, test, formazione e supporto applicativo, utilizzando dati realistici ma non riconducibili direttamente agli interessati;
- garantisce che le operazioni di data masking avvengano secondo procedure documentate, con ruoli e responsabilità chiari e con adeguata protezione delle chiavi o delle logiche di ricostruzione;

- assicura la gestione del **diritto all'oblio** (cancellazione/anonimizzazione) dei dati personali su richiesta dell'interessato o decorso il termine di conservazione, mediante procedure che prevedono la cancellazione o l'anonimizzazione sicura nei sistemi applicativi, nei database, nei backup (nel limite del tecnicamente possibile) e nelle copie di test, tenendo conto degli obblighi di conservazione di legge;
- integra questi aspetti nei processi di progettazione e sviluppo (privacy by design e by default) e nei rapporti contrattuali con clienti e fornitori.

---

7. Gestione BYOD (Bring Your Own Device) e lavoro da remoto

UNITIVA riconosce la diffusione di dispositivi personali utilizzati per fini lavorativi (**BYOD**) e la possibilità di lavoro da remoto come fattori che impattano sulla sicurezza dei dati.

A tal fine:

- l'utilizzo di dispositivi personali (smartphone, laptop, tablet, storage esterni) per l'accesso a sistemi e dati aziendali è **espressamente regolato da policy e procedure**;
- l'accesso ai sistemi da BYOD è concesso solo previa autorizzazione, verifica dei requisiti minimi di sicurezza del dispositivo e accettazione delle regole di utilizzo da parte dell'utente;
- sono previsti controlli tecnici quali cifratura dei dati, autenticazione forte, gestione da remoto (MDM/MAM ove applicabile), blocco schermo, aggiornamenti di sicurezza, protezione anti-malware;
- è vietata la memorizzazione non autorizzata di informazioni aziendali su dispositivi personali o applicazioni non approvate;
- per il lavoro da remoto vengono definiti requisiti minimi di sicurezza relativi a connessioni, ambienti di lavoro, reti domestiche, uso di VPN e protezione delle credenziali.

---

8. Sicurezza delle postazioni di lavoro, protezione della scrivania e dei PC

UNITIVA adotta il principio di **"clean desk & clear screen"** per ridurre il rischio di accesso non autorizzato a informazioni e sistemi.

In particolare, tutto il personale è tenuto a:

- mantenere le scrivanie libere da documenti contenenti informazioni riservate quando non sono necessari e, in ogni caso, a fine giornata;
- conservare documenti cartacei e supporti rimovibili (USB, hard disk esterni, ecc.) in armadi o contenitori chiusi a chiave quando non utilizzati;
- bloccare lo schermo del PC, laptop o dispositivo quando ci si allontana dalla postazione, anche per brevi periodi;
- non annotare password in chiaro su fogli, taccuini o post-it accessibili a terzi;
- utilizzare esclusivamente software autorizzato, mantenendo i dispositivi aggiornati e protetti;

- segnalare tempestivamente al RSGSD o al referente IT eventuali anomalie, malware sospetti o incidenti di sicurezza.

La sicurezza delle postazioni di lavoro e dei PC è supportata da misure tecniche (es. cifratura, antivirus, aggiornamenti, restrizioni di installazione software) e da regole organizzative disciplinate nelle policy e procedure interne.

---

9. SICUREZZA DELLE INFRASTRUTTURE FISICHE ED AMBIENTALI

UNITIVA si impegna a proteggere le proprie **infrastrutture fisiche ed ambientali** (sede, locali tecnici, data center di terze parti, apparati di rete, sistemi di alimentazione, climatizzazione) da accessi non autorizzati, danneggiamenti, eventi ambientali e malfunzionamenti.

In particolare:

- l'accesso ai locali dove sono collocate apparecchiature critiche è controllato e consentito solo a personale autorizzato;
- sono adottate misure per la protezione di dispositivi e cablaggi (armadi rack chiusi, dispositivi fisicamente protetti, controllo delle prese di rete accessibili);
- sono previste soluzioni idonee a mitigare rischi legati a incendio, allagamento, sbalzi di tensione, condizioni ambientali non idonee;
- i fornitori di servizi di data center e cloud sono selezionati e gestiti tenendo conto dei controlli fisici ed ambientali adottati, anche in ottica di continuità operativa;
- le misure fisiche ed ambientali sono integrate con il **piano di Business Continuity & Disaster Recovery**, che definisce tempi obiettivo di ripristino (RTO/RPO) e modalità operative per garantire la continuità dei servizi critici.

---

10. GESTIONE DEGLI INCIDENTI, CONTINUITÀ OPERATIVA E MIGLIORAMENTO

UNITIVA adotta procedure specifiche per:

- la **gestione degli incidenti di sicurezza** (rilevazione, analisi, contenimento, notifica, ripristino, lesson learned);
- la **continuità operativa** e il **disaster recovery**, in linea con i requisiti del SGSD, gli obblighi contrattuali verso i clienti e il contesto organizzativo;
- la gestione di **non conformità, azioni correttive e azioni di miglioramento**, con monitoraggio dell'efficacia delle misure adottate.

Tutto il personale è tenuto a **segnalare immediatamente** qualsiasi incidente o sospetto tale (furto o smarrimento dispositivi, accessi non autorizzati, malware, perdita di dati, anomalie di sistema) secondo i canali definiti.

11. CONSAPEVOLEZZA, FORMAZIONE E COMUNICAZIONE

UNITIVA ritiene fondamentale la **formazione continua** e la **consapevolezza** del personale sui temi della sicurezza dei dati.

A tal fine la Direzione si impegna a:

- garantire che le competenze necessarie alla gestione sicura dei dati siano identificate, sviluppate e mantenute;
- programmare periodicamente attività di formazione e sensibilizzazione (onboarding, aggiornamenti periodici, comunicazioni interne, campagne di awareness);
- assicurare che tutto il personale conosca la presente Politica, le policy di dettaglio e le procedure ad esso applicabili;
- utilizzare canali di comunicazione idonei (riunioni, email, intranet, bacheche, strumenti collaborativi) per diffondere informazioni rilevanti in materia di sicurezza dei dati, privacy e continuità operativa.

12. RUOLI, RESPONSABILITÀ E OSSERVANZA

L'osservanza della presente Politica è responsabilità di:

- **tutto il personale** che, a qualsiasi titolo, collabora con l'azienda o tratta informazioni rientranti nel campo di applicazione del SGSD;
- **tutte le terze parti** che intrattengono rapporti con l'azienda e hanno accesso a dati, sistemi o infrastrutture di UNITIVA.

Il **Responsabile del Sistema di Gestione della Sicurezza dei Dati (RSGSD)** ha il compito di:

- coordinare l'analisi e il trattamento dei rischi relativi alla sicurezza dei dati;
- definire, proporre e aggiornare norme, policy e procedure di sicurezza;
- monitorare l'efficacia delle misure di sicurezza e proporre azioni di miglioramento;
- coordinare audit interni, attività di monitoraggio e azioni correttive;
- promuovere formazione e consapevolezza del personale.

Ogni violazione intenzionale o dovuta a negligenza delle regole di sicurezza può comportare provvedimenti disciplinari e, ove necessario, azioni legali, nel rispetto delle leggi e dei contratti applicabili.

13. RIESAME E AGGIORNAMENTO DELLA POLITICA

La presente Politica è **riesaminata periodicamente** dalla Direzione, almeno una volta l'anno e, comunque, in occasione di:

- cambiamenti significativi nel contesto organizzativo, tecnologico, normativo o di business;
- risultati di audit interni o esterni;

- incidenti di sicurezza rilevanti o cambiamenti significativi nel profilo di rischio;
- aggiornamenti delle norme di riferimento (es. ISO/IEC 27001, provvedimenti del Garante, altre normative cogenti).

Il riesame verifica:

- la coerenza della Politica con gli indirizzi strategici aziendali;
- l'adeguatezza rispetto ai rischi attuali e alle esigenze delle parti interessate;
- l'efficacia delle misure di sicurezza implementate e degli obiettivi fissati.

Gli esiti del riesame sono documentati e possono comportare l'aggiornamento della Politica, dei relativi obiettivi e del programma di gestione.

---

14. Impegno della Direzione

La Direzione di UNITIVA S.r.l.:

- **approva** la presente Politica;
- garantisce la disponibilità delle risorse necessarie per l'attuazione, il mantenimento e il miglioramento continuo del SGSD;
- promuove attivamente la cultura della sicurezza dei dati in tutta l'organizzazione;
- assicura che i ruoli e le responsabilità relativi alla sicurezza dei dati siano chiaramente definiti, comunicati e compresi;
- sostiene tutte le iniziative e i progetti orientati al miglioramento dei livelli di sicurezza e alla protezione delle informazioni proprie e dei clienti.

Luogo, data
Napoli, 01.09.2025

La Direzione
UNITIVA S.r.l.