POLITICA PER LA SICUREZZA DELLE INFORMAZIONI
ISMS DOC 5.2-01

Premesso che **J+S**, nello svolgimento delle proprie attività di **progettazione, direzione lavori, coordinamento della sicurezza in fase di progettazione ed esecuzione, produce, riceve, conserva e tratta informazioni tecniche e gestionali ad elevato valore e criticità**, tra cui elaborati di progetto, relazioni di calcolo, risultati di indagini, documentazione di sicurezza e atti contrattuali.

Tali informazioni, per la natura delle opere trattate possono richiedere livelli di protezione particolarmente elevati. La **compromissione della riservatezza** può determinare divulgazione non autorizzata di soluzioni tecniche, dati sensibili di infrastrutture e know-how; la **perdita di integrità** (alterazioni, errori, versioni non controllate) può generare decisioni tecniche errate, non conformità e rischi per la sicurezza dell'opera; la **mancata disponibilità** (indisponibilità di documenti e dati nei momenti critici di consegna, cantiere o ispezione) può causare ritardi, contenziosi, penali contrattuali e blocchi operativi.

Inoltre, una parte delle informazioni trattate include **dati personali** (dipendenti, collaboratori, fornitori, referenti dei clienti) e, ove applicabile, dati con particolare necessità di tutela; la loro gestione richiede misure adeguate a garantire un trattamento conforme e sicuro lungo l'intero ciclo di vita informativo.

Alla luce di quanto sopra, la Direzione riconosce che la sicurezza delle informazioni è un fattore determinante per la **sostenibilità aziendale**, la tutela della reputazione, il rispetto degli obblighi contrattuali e normativi e la continuità operativa, e costituisce un presupposto essenziale per assicurare affidabilità e qualità dei servizi resi su opere e infrastrutture.

La Direzione, responsabile ultima della sicurezza delle informazioni, ha delegato i responsabili delle divisioni interne ad attuare quanto necessario, in accordo con il responsabile dei sistemi IT, il responsabile della sicurezza e l'amministrazione.

Tutto il personale che, a qualsiasi titolo, collabora con l'azienda è responsabile dell'osservanza dalla presente politica e della segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

La Direzione ha deciso di adottare e mantenere un **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI/ISMS)**, con l'obiettivo di assicurare un livello di protezione adeguato al valore delle informazioni trattate e ai rischi correlati, indipendentemente dal formato (digitale o cartaceo) e dal contesto di utilizzo (sede, cantieri/sopralluoghi, lavoro da remoto, collaborazione con clienti, fornitori, partner e consulenti).

La Direzione riconosce che la tutela della sicurezza delle informazioni costituisce un fattore abilitante per:

- la qualità e l'affidabilità dei servizi resi ai clienti;
- il rispetto di obblighi contrattuali e normativi (inclusi, ove applicabile, i principi di sicurezza e riservatezza nel trattamento dei dati personali);

J+S S.p.A.
Via dei Mestieri 13 – Concorezzo (MB) 20863 – Italy
Pec: segreteria@pec.jpius.it
P.IVA & C.F. 02280620960
+39 039 6886381 – info@jpius.it – jpius.it

- la protezione del know-how aziendale e la continuità operativa;
- la fiducia di clienti, partner e altre parti interessate.

J+S rende nota la presente Politica e la comunica a tutto il personale mediante strumenti interni (intranet, bacheca e/o canali equivalenti), assicurandone l'accessibilità e la comprensione. La Politica è inoltre resa disponibile alle parti interessate esterne, ove appropriato, tramite pubblicazione sul sito web o altri canali concordati.

Impegni della Direzione

La Direzione, consapevole del proprio ruolo di responsabilità ultima in materia di sicurezza delle informazioni, si impegna a:

1. **Conformità e requisiti applicabili:** Garantire livelli di sicurezza adeguati a rispettare gli obblighi applicabili (legali, regolatori e contrattuali) e i requisiti specifici concordati con clienti e partner.
2. **Miglioramento continuo:** Migliorare in modo continuo l'efficacia del SGSI, attraverso obiettivi misurabili, audit, riesami periodici e piani di miglioramento.
3. **Gestione del rischio;** Identificare, valutare e trattare i rischi per la sicurezza delle informazioni, eliminandoli o riducendoli a livelli accettabili ove tecnicamente possibile ed economicamente sostenibile, in coerenza con l'appetito al rischio definito dalla Direzione.
4. **Controllo degli accessi e principio di necessità:** Rendere disponibili le informazioni e gli strumenti di lavoro solo a chi ne ha effettiva necessità per lo svolgimento delle proprie mansioni, applicando il principio del **need-to-know** e la concessione dei privilegi minimi necessari (**least privilege**), con autorizzazioni e revoche tracciabili.
5. **Protezione del patrimonio informativo e del know-how:** Salvaguardare la riservatezza e l'integrità delle informazioni strategiche aziendali, incluse metodologie, elaborati, librerie, template e, ove presenti, **codice sorgente** e applicativi interni, prevenendo divulgazioni non autorizzate e uso improprio.
6. **Continuità operativa e resilienza:** Assicurare adeguate misure di continuità e ripristino (es. backup, test di restore, gestione incidenti) per garantire la disponibilità delle informazioni e dei servizi essenziali, in particolare nei periodi critici di consegna e nelle commesse con vincoli contrattuali.
7. **Formazione, consapevolezza e comportamento:** Formare e sensibilizzare il personale e i collaboratori sui rischi e sulle regole di sicurezza, promuovendo comportamenti responsabili e verificando il rispetto dei principi etici e delle regole operative interne (inclusa la segnalazione tempestiva di anomalie e incidenti).
8. **Gestione dei fornitori e dei partner:** Selezionare e gestire fornitori e partner tenendo conto della loro capacità di conformarsi ai requisiti di sicurezza dell'Organizzazione; definire in fase contrattuale requisiti minimi (es. protezione accessi, tracciabilità, gestione incidenti, livelli di servizio) e verificarne l'applicazione in modo proporzionato alla criticità del servizio.

9. **Requisiti di sicurezza nei servizi erogati:** Fornire servizi per i quali i requisiti di sicurezza siano definiti in modo chiaro (quando applicabile, già in fase di offerta e contratto), inclusi canali autorizzati di scambio, criteri di protezione e regole di conservazione e tracciabilità.

10. **Politiche per la privacy:** Facilitare la conformità al GDPR e ad altre normative sulla protezione dei dati, mediante il rispetto dei diritti degli interessati e la gestione di eventuali incidenti di sicurezza che coinvolgono PII

Ruoli, responsabilità e attuazione

La Direzione delega ai responsabili delle funzioni/divisioni interne l'attuazione delle misure necessarie nei rispettivi ambiti, in coordinamento con il **Responsabile IT**, con il **Responsabile della Sicurezza delle Informazioni** (ove previsto) e con l'Amministrazione, garantendo che ruoli e responsabilità siano definiti, comunicati e riesaminati periodicamente.

Tutto il personale e chiunque collabori a qualsiasi titolo con l'Organizzazione è tenuto a:

- rispettare la presente Politica e le procedure/istruzioni applicabili;
- utilizzare correttamente strumenti e credenziali assegnate;
- segnalare tempestivamente eventi, anomalie, sospetti di violazione o incidenti (anche se non ancora formalmente classificati), contribuendo alla gestione e al miglioramento del SGSI.

Comunicazione, riesame e aggiornamento

La presente Politica è **documentata, approvata dalla Direzione, comunicata** e mantenuta disponibile come informazione documentata; viene inoltre **riesaminata periodicamente** e aggiornata in caso di cambiamenti significativi (organizzazione, tecnologie, fornitori, requisiti cliente/PA, minacce, incidenti)

Concorezzo, 01/12/2025

La Direzione