PSGSI

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

R	Data	Descrizione
00	01/09/2026	Prima emissione

Redazione (ASI)	Verifica (AQ)	Approvazione (DIR)
x	x	x

Questo documento definisce la Politica per la sicurezza delle informazioni di IDATA GROUP e gli indirizzi della Direzione per la protezione delle informazioni aziendali e di quelle affidate dai clienti.

IDATA GROUP opera nei servizi ICT e nelle attività di consulenza, progettazione, sviluppo e supporto tecnico. Le attività comprendono soluzioni software, anche web e mobile, e progetti negli ambiti delle telecomunicazioni, delle reti, del cloud, della cybersecurity, dell'Internet of Things, dell'analisi dati, insieme a iniziative di ricerca e innovazione svolte anche con partner tecnologici, università ed enti di ricerca.

La sicurezza delle informazioni è essenziale per pianificare, sviluppare e realizzare le commesse, collaborare con clienti e partner e proteggere i risultati dei progetti. IDATA GROUP tutela le informazioni durante la definizione delle offerte, la progettazione e lo sviluppo delle soluzioni, l'esecuzione delle attività tecniche e la gestione dei servizi. La protezione riguarda sia gli ambienti aziendali sia le informazioni e le risorse dei clienti cui il personale accede nell'ambito degli incarichi autorizzati, anche da remoto.

L'obiettivo primario è proteggere i dati e le informazioni, il know-how, il software, la documentazione tecnica e progettuale e la proprietà intellettuale di IDATA GROUP e dei clienti. La protezione comprende inoltre i dati commerciali, economici e di commessa e i dati personali di dipendenti, collaboratori, candidati e altri interessati.

La fiducia dei clienti, il rispetto degli impegni contrattuali e la qualità delle prestazioni dipendono anche dalla capacità di preservare la riservatezza, l'integrità e la disponibilità delle informazioni lungo l'intero ciclo di vita delle attività e dei servizi.

La presente Politica stabilisce gli indirizzi per gestire la sicurezza delle informazioni sotto il profilo organizzativo, tecnico e fisico, con misure proporzionate ai rischi e coerenti con il campo di applicazione del SGSI. Gli indirizzi si applicano ai processi operativi e di supporto, ai sistemi aziendali e alle attività svolte presso i clienti o da remoto.

La gestione della sicurezza delle informazioni di IDATA GROUP comprende:

- l'identificazione e la classificazione delle informazioni, degli asset e delle attività critiche per i servizi e le commesse;
- la valutazione e il trattamento dei rischi, con responsabilità definite e accettazione del rischio residuo;
- la sicurezza dei sistemi, delle reti e del ciclo di sviluppo, rilascio e manutenzione del software;
- la gestione delle vulnerabilità, degli aggiornamenti, degli eventi e degli incidenti di sicurezza;
- la gestione delle identità, delle autorizzazioni e degli accessi fisici, logici e remoti;
- la protezione dei dati personali e il rispetto dei requisiti legali, normativi e contrattuali applicabili, inclusi GDPR e requisiti NIS2 ove applicabili;
- la continuità delle attività, i backup e la verifica del ripristino delle informazioni e dei servizi;
- la gestione dei rischi dei fornitori, dei partner e dei servizi esterni, inclusi cloud e posta elettronica.

IDATA GROUP integra la sicurezza nella progettazione delle soluzioni e nell'organizzazione delle commesse, dalla raccolta dei requisiti al rilascio e alla manutenzione. Protegge codice, documentazione, dati e credenziali dei progetti, controlla le modifiche e gli accessi agli ambienti di sviluppo, prova ed esercizio e rispetta le regole di sicurezza concordate con i clienti.

IDATA GROUP pianifica la continuità delle attività e il recupero dei servizi in relazione alle esigenze operative, ai rischi e agli impegni contrattuali, per limitare gli effetti di guasti, incidenti e interruzioni su clienti e altre parti interessate.

A tale scopo IDATA GROUP adotta un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) coerente con la ISO/IEC 27001 e ne promuove il miglioramento continuo, integrando la sicurezza nella gestione dei processi e delle commesse.

La Politica costituisce il quadro di riferimento per definire e riesaminare obiettivi di sicurezza misurabili, con responsabili, risorse, scadenze e indicatori, orientati a:

- proteggere le informazioni aziendali e dei clienti e prevenire accessi o divulgazioni non autorizzati;
- sostenere la continuità dei servizi ICT e il rispetto degli impegni assunti nelle commesse;
- tutelare il know-how, la proprietà intellettuale e l'affidabilità dei risultati progettuali;
- soddisfare i requisiti applicabili e migliorare l'efficacia dei controlli di sicurezza.

La Direzione di IDATA GROUP si impegna a fornire le risorse e le competenze necessarie, ad assegnare ruoli e responsabilità e a sostenere l'attuazione e il miglioramento continuo del SGSI. Nell'ambito delle attività e dei servizi inclusi nel sistema, IDATA GROUP assume i seguenti impegni:

- proteggere la riservatezza mediante la classificazione delle informazioni, gli obblighi di riservatezza, la condivisione controllata e l'accesso ai soli soggetti autorizzati, con particolare attenzione ai dati dei clienti e alla documentazione di progetto;
- preservare l'integrità di dati, software, configurazioni e documenti mediante autorizzazioni coerenti con i ruoli, controllo delle modifiche, verifiche dei risultati e tracciabilità delle operazioni rilevanti;
- assicurare la disponibilità richiesta alle attività mediante manutenzione, monitoraggio, backup, prove di ripristino e misure di continuità commisurate alla criticità dei servizi e ai tempi concordati con i clienti;
- definire e comunicare a dipendenti, collaboratori, fornitori e partner gli obblighi di sicurezza pertinenti ai rispettivi incarichi, inclusi quelli relativi alle informazioni e alle risorse dei clienti;
- autorizzare, controllare e monitorare gli accessi fisici e informatici secondo i seguenti criteri:
  - (a) consentire l'accesso alle sole informazioni necessarie all'incarico, secondo il principio della necessità di sapere;
  - (b) assegnare i privilegi minimi necessari al ruolo, riesaminarli e revocarli quando cambiano o cessano le esigenze di accesso;
  - (c) proteggere sedi, locali tecnici e accessi remoti e rispettare le autorizzazioni e le regole definite per gli ambienti dei clienti;
- rendere ogni dipendente, collaboratore e terza parte consapevole del proprio ruolo e degli effetti delle proprie azioni sulla sicurezza delle informazioni;
- assicurare formazione e sensibilizzazione adeguate ai ruoli, ai rischi e alle attività svolte, incluse le attività da remoto e presso i clienti;
- gestire le informazioni proprie e quelle affidate dai clienti nel rispetto dei requisiti applicabili, delle istruzioni ricevute e degli accordi contrattuali, proteggendo i dati personali e i diritti degli interessati;
- applicare controlli proporzionati al valore delle informazioni e ai rischi, anche per dispositivi portatili, trasferimenti di dati, servizi cloud e risorse affidate a terzi;
- richiedere a tutto il personale IDATA GROUP, nell'ambito delle proprie competenze, di:
  - (a) rispettare i requisiti legali, contrattuali e organizzativi applicabili alle attività svolte;

(b) proteggere riservatezza, integrità e disponibilità delle informazioni e della proprietà intellettuale di IDATA GROUP, dei clienti e dei partner;

(c) utilizzare con cura e secondo le regole autorizzate dispositivi, sistemi, account e altre risorse assegnate;

(d) custodire, condividere e trasferire dati e documenti di lavoro solo mediante strumenti e modalità autorizzati;

(e) segnalare tempestivamente eventi, anomalie e violazioni di sicurezza, anche sospette, attraverso i canali aziendali previsti;

(f) segnalare esigenze di aggiornamento delle procedure e opportunità di miglioramento. Nei limiti delle responsabilità e delle deleghe assegnate, il personale deve inoltre:

(g) applicare la Politica e le procedure di sicurezza pertinenti al proprio incarico;

(h) richiedere gli accessi necessari alle proprie attività attraverso il processo autorizzativo definito;

(i) verificare gli impegni di riservatezza e sicurezza richiesti alle terze parti coinvolte nelle attività di competenza;

(l) operare nel rispetto delle decisioni di trattamento e delle condizioni di accettazione del rischio del proprio ambito.

- richiedere al personale con responsabilità specifiche nella gestione della sicurezza delle informazioni di:

  (a) attuare le misure previste dalle politiche di sicurezza di IDATA GROUP;

  (b) verificare il rispetto dei requisiti e delle procedure del SGSI e gestire le non conformità rilevate;

  (c) mantenere aggiornati gli inventari e monitorare i controlli sugli asset e sui servizi di competenza;

  (d) coordinare l'attuazione dei controlli organizzativi, fisici e tecnologici per le attività interne, le commesse e le risorse affidate a terzi;

  (e) informare e formare personale e terze parti sulle regole pertinenti e sulle conseguenze del loro mancato rispetto;

  (f) verificare l'efficacia delle misure adottate e proporre gli interventi necessari;

  (g) riesaminare i rischi del proprio ambito e seguire l'avanzamento delle azioni di trattamento;

  (h) mantenere operative le misure di risposta agli incidenti e di continuità e verificarne l'adeguatezza mediante prove e riesami.

- considerare nel riesame del contesto i fattori esterni che possono influire sulla sicurezza e sulla continuità, inclusi, quando rilevanti, eventi climatici e ambientali e dipendenze da sedi, connettività e fornitori;

- definire, per le terze parti che accedono alle informazioni o alle risorse di IDATA GROUP e dei clienti, impegni contrattuali proporzionati ai rischi, che prevedano di:

(a) formalizzare gli obblighi di riservatezza e non divulgazione delle informazioni trattate;

(b) proteggere dati, risorse e proprietà intellettuale utilizzati nello svolgimento delle attività assegnate;

(c) rispettare i requisiti di sicurezza concordati e comunicare tempestivamente gli incidenti che possono incidere sulle informazioni o sui servizi affidati.

IDATA GROUP persegue la certificazione del SGSI secondo la ISO/IEC 27001 e, dopo il suo conseguimento, il relativo mantenimento, attraverso verifiche indipendenti e il miglioramento continuo del sistema.

La Politica si applica alle informazioni, ai processi, alle persone, ai sistemi e alle sedi compresi nel campo di applicazione formalizzato del SGSI, incluse le attività svolte da remoto o presso i clienti. È vincolante per la Direzione, i dipendenti e i collaboratori e, per quanto di competenza, per i fornitori, i partner e le altre terze parti coinvolte.

La Direzione comunica la Politica al personale e la rende disponibile alle parti interessate pertinenti. Ne riesamina almeno annualmente l'idoneità, e in occasione di cambiamenti significativi, considerando evoluzione del business, rischi, requisiti, incidenti ed esiti degli audit. Il riesame comprende gli obiettivi di sicurezza, i risultati ottenuti e le risorse necessarie al miglioramento del SGSI.