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

Storia della versione

Versione	Data	Autore	Approvato da
1	28/04/2026	Glauco Timoteo	William Palozzo

Indice

Scopo

La presente politica ha lo scopo di definire, assegnare e comunicare in modo chiaro e univoco i ruoli, le responsabilità e le autorità in materia di sicurezza delle informazioni all'interno di DG Impianti Industriali S.p.A. Attraverso una mappatura dettagliata che collega ogni funzione aziendale ai propri doveri di protezione degli asset informativi, il documento garantisce che tutti gli aspetti del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) siano gestiti, supervisionati e mantenuti in conformità con i requisiti normativi applicabili.

Questa politica si integra con la struttura organizzativa formale dell'azienda, così come rappresentata nel *MOD Organigramma* e nel *MOD Mansionario* , affinché le responsabilità di sicurezza siano parte integrante delle mansioni quotidiane di tutto il personale e non siano percepite come attività accessorie o separate dal contesto operativo.

Campo di applicazione

Questa politica si applica a tutte le funzioni aziendali di DG Impianti Industriali S.p.A., presso la sede legale di Via Napo Torriani n.22, Milano, e la sede operativa di Via Antonio Vivaldi n.4, Montesilvano (PE). Essa coinvolge l'intero personale — dipendenti, collaboratori e dirigenti — nonché le parti interessate esterne, quali fornitori, appaltatori e partner contrattuali, che interagiscono con le informazioni e le risorse informative dell'organizzazione.

Il campo di applicazione comprende tutte le infrastrutture fisiche e logiche, i sistemi informativi, le reti di telecomunicazione e gli asset informativi gestiti dall'organizzazione, indipendentemente dal formato in cui le informazioni sono conservate o trasmesse.

Riferimenti normativi

- **ISO 27001:2022:** Requisiti per i sistemi di gestione della sicurezza delle informazioni.
- **ISO 27002:2022:** Linee guida per i controlli di sicurezza delle informazioni.
- **Regolamento (UE) 2016/679 (GDPR):** Protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Termini e definizioni

- **SGSI (Sistema di Gestione della Sicurezza delle Informazioni):** Parte del sistema di gestione complessivo, basata su un approccio al rischio aziendale, finalizzata a stabilire, implementare, operare, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **Sicurezza delle Informazioni:** La tutela della riservatezza, integrità e disponibilità delle informazioni.

- **Top Management:** Persona o gruppo di persone che dirige e controlla un'organizzazione al livello più alto; in DG Impianti Industriali S.p.A. è costituito dal Chief Executive Officer e dal Managing Director.
- **Rischio per la sicurezza delle informazioni:** Potenziale che una data minaccia sfrutti le vulnerabilità di un asset o di un gruppo di asset, causando un danno all'organizzazione.
- **RSGSI (Responsabile del Sistema di Gestione della Sicurezza delle Informazioni):** Figura nominata dal Top Management con l'autorità e la responsabilità di coordinare il SGSI e di riferire sulle sue prestazioni.

Ruoli e responsabilità

La sicurezza delle informazioni in DG Impianti Industriali S.p.A. è una responsabilità condivisa che attraversa l'intera struttura organizzativa, dal vertice aziendale fino alle funzioni operative e alle terze parti. I ruoli di seguito descritti sono coerenti con la macrostruttura formalizzata nel *MOD Organigramma* e con le mansioni dettagliate nel *MOD Mansionario* .

- **Chief Executive Officer** : Approva la politica per la sicurezza delle informazioni, garantisce la disponibilità delle risorse necessarie per il SGSI e assicura l'integrazione dei relativi requisiti nei processi strategici dell'organizzazione.
- **Managing Director** : Supervisiona l'attuazione operativa delle misure di sicurezza delle informazioni, nomina formalmente il RSGSI e promuove una cultura della sicurezza a tutti i livelli aziendali.
- **ICT-RSGSI** : Assicura che il SGSI sia stabilito, attuato e mantenuto in conformità alla norma ISO 27001, coordina la valutazione del rischio informatico e la gestione degli incidenti, riferisce al Top Management sulle prestazioni del sistema e gestisce i controlli tecnici sull'infrastruttura IT e di telecomunicazione.
- **HSEQ** : Supporta il mantenimento del Sistema di Gestione Integrato curando la documentazione, gli audit interni e la gestione delle non conformità, collaborando con il RSGSI per gli aspetti di sovrapposizione tra sicurezza delle informazioni e sistemi qualità, salute, sicurezza e ambiente.
- **HR** : Integra le responsabilità di sicurezza delle informazioni nei processi di assunzione, inserimento e cessazione del rapporto di lavoro, garantisce la pianificazione e l'erogazione della formazione in materia di sicurezza e applica le procedure disciplinari in caso di violazione delle politiche.
- **Gen. Services \ T&A** : Garantisce il supporto logistico e amministrativo necessario alla protezione fisica delle sedi, alla gestione dell'accoglienza di visitatori e ospiti e all'archiviazione della documentazione amministrativa nel rispetto delle regole di sicurezza.
- **NDA\Contract Evaluation** : Esamina e valuta gli accordi di non divulgazione e i documenti contrattuali, assicurando che le clausole di riservatezza e i requisiti di sicurezza delle informazioni siano adeguatamente inclusi negli impegni con terze parti.

- **Tutto il personale (dipendenti e collaboratori)** : Rispetta la presente politica e tutte le politiche e procedure di sicurezza correlate, segnala tempestivamente qualsiasi incidente, anomalia o debolezza osservata e adotta le misure pratiche per proteggere le informazioni e le risorse aziendali.
- **Terze parti (fornitori, appaltatori, partner)** : Mantengono la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi di cui sono responsabili, in conformità con le politiche aziendali e gli accordi contrattuali sottoscritti.

Definizione dei ruoli e responsabilità

La seguente matrice costituisce la mappatura dettagliata delle responsabilità in materia di sicurezza delle informazioni per ciascun ruolo aziendale. Essa integra quanto formalizzato nel *MOD Mansionario* con gli obblighi specifici derivanti dal SGSI, garantendo che i doveri di protezione degli asset informativi siano parte integrante delle mansioni quotidiane.

Responsabilità del Top Management

Ruolo	Responsabilità in materia di sicurezza delle informazioni
Chief Executive Officer	Approva la politica per la sicurezza delle informazioni e le politiche specifiche per argomento. Garantisce che le risorse umane, tecnologiche ed economiche necessarie per il SGSI siano allocate. Approva la struttura organizzativa formalizzata nel *MOD Organigramma* . Supervisiona la risposta agli incidenti di sicurezza rilevanti, minimizzando l'impatto sul business. Promuove il miglioramento continuo del SGSI nell'ambito del riesame della direzione.
Managing Director	Nomina formalmente il RSGSI, definendone poteri e responsabilità. Supervisiona l'attuazione delle misure di gestione dei rischi di sicurezza informatica. Assicura l'integrazione dei requisiti del SGSI nei processi operativi dell'organizzazione. Richiede a tutto il personale sotto la propria direzione di applicare le politiche e le procedure di sicurezza. Riceve e analizza i rapporti sulle prestazioni del SGSI forniti dal RSGSI.

Responsabilità delle funzioni di supporto

Ruolo	Responsabilità in materia di sicurezza delle informazioni
ICT-RSGSI	Assicura che i processi del SGSI siano stabiliti, attuati e mantenuti in conformità alla norma ISO 27001. Riferisce al Top Management sull'andamento del SGSI e su ogni esigenza di miglioramento. Coordina il processo di valutazione del rischio informatico e gestisce la relativa documentazione. Coordina lo sviluppo e la manutenzione delle politiche e degli standard di sicurezza. Funge da punto di contatto per audit interni, esterni e per le autorità competenti. Gestisce le infrastrutture informatiche e di telecomunicazione, garantendone il corretto funzionamento e la sicurezza. Implementa e gestisce i controlli tecnici del SGSI, inclusi backup, protezione da minacce esterne e gestione degli accessi logici. Supervisiona la gestione degli incidenti di sicurezza informatica fino alla loro risoluzione. Esegue valutazioni del rischio tecnico e test di vulnerabilità. Gestisce i sistemi di controllo degli accessi fisici alle aree contenenti asset informativi critici.

HR	Formalizza e mantiene aggiornati il *MOD Organigramma* e il *MOD Mansionario* , integrando le responsabilità per la sicurezza delle informazioni in ogni ruolo. Implementa le verifiche di sicurezza nelle fasi di assunzione, inserimento e cessazione del rapporto di lavoro, assicurando la tempestiva concessione, modifica o revoca degli accessi in collaborazione con ICT-RSGSI. Garantisce la pianificazione e l'erogazione della formazione continua sulla sicurezza delle informazioni. Gestisce la riservatezza e la protezione dei dati personali dei dipendenti in conformità al GDPR. Applica le procedure disciplinari in caso di violazione delle politiche di sicurezza.
HSEQ	Supporta il mantenimento della documentazione del Sistema di Gestione Integrato, assicurando la coerenza tra i requisiti HSEQ e quelli di sicurezza delle informazioni. Gestisce gli audit interni periodici in coordinamento con il RSGSI. Coordina la gestione delle non conformità e delle azioni correttive in materia di sicurezza. Collabora con il Top Management nella valutazione del rischio organizzativo e nella gestione delle azioni di mitigazione.
NDA\Contract Evaluation	Esamina e valuta gli accordi di non divulgazione e i contratti con terze parti, assicurando l'inclusione di clausole adeguate a tutela della riservatezza e della sicurezza delle informazioni. Identifica e mitiga i rischi contrattuali associati al trattamento di informazioni da parte di soggetti esterni. Fornisce supporto nella definizione dei requisiti di sicurezza da inserire nei contratti con clienti, fornitori e partner.
Gen. Services \ T&A	Garantisce il supporto logistico alla sicurezza fisica delle sedi, inclusa la gestione dell'accoglienza di ospiti e visitatori secondo le procedure di controllo degli accessi. Assicura la corretta gestione

	della documentazione amministrativa e dei servizi di archiviazione in conformità alle regole di protezione delle informazioni. Coordina i servizi generali in modo coerente con le politiche di sicurezza fisica e ambientale.

Responsabilità delle funzioni di linea e operative

Ruolo	Responsabilità in materia di sicurezza delle informazioni
Project Management Office	Assicura che le metodologie e gli standard di gestione dei progetti includano i requisiti di sicurezza delle informazioni applicabili. Monitora la conformità dei progetti alle politiche di sicurezza, segnalando eventuali scostamenti al RSGSI.
Project Management Services	Garantisce che la documentazione di progetto sia gestita nel rispetto delle regole di classificazione ed etichettatura delle informazioni. Assicura che gli obblighi contrattuali di riservatezza con i clienti siano rispettati durante l'esecuzione delle commesse.
Project Engineering	Tutela la riservatezza e l'integrità della documentazione tecnica di progetto, delle specifiche e dei rapporti ingegneristici. Garantisce il rispetto delle politiche di sicurezza nello scambio di informazioni tecniche con clienti, fornitori e discipline interne.
Commercial	Gestisce le informazioni commerciali riservate relative a offerte, gare e relazioni con i clienti in conformità con le politiche di classificazione delle informazioni. Assicura la protezione dei dati sensibili nelle fasi pre-contrattuali e contrattuali.
Workload	Protegge le informazioni relative all'allocazione delle risorse e ai carichi di lavoro, assicurando che i dati operativi

	siano accessibili esclusivamente al personale autorizzato.
R&D & Innovation	Garantisce la protezione della proprietà intellettuale e dei risultati della ricerca, applicando le misure di sicurezza previste per le informazioni classificate come riservate o confidenziali.
Sustainability	Gestisce le informazioni relative alle prestazioni ESG e alla conformità ambientale nel rispetto delle politiche di sicurezza, assicurando che i dati sensibili siano trattati in modo adeguato.

Responsabilità di tutto il personale e delle terze parti

Ogni dipendente e collaboratore di DG Impianti Industriali S.p.A. deve rispettare la presente politica e tutte le politiche e le procedure di sicurezza correlate, con particolare riguardo alla *POL Politica di sicurezza delle informazioni* e alla *POL Politica di classificazione ed etichettatura delle informazioni* . Ciascun membro del personale deve segnalare tempestivamente qualsiasi incidente, anomalia o debolezza di sicurezza osservata attraverso i canali ufficiali definiti dal RSGSI e deve adottare tutte le misure pratiche necessarie per proteggere le informazioni e le risorse aziendali da accessi non autorizzati, furti o danni.

Le terze parti che accedono alle informazioni o ai sistemi dell'organizzazione — inclusi fornitori, appaltatori, consulenti e partner — devono mantenere la riservatezza, l'integrità e la disponibilità delle informazioni e dei sistemi di cui sono responsabili, in piena conformità con le politiche aziendali e con gli accordi contrattuali sottoscritti, come disciplinato dalla *PRO Procedura di gestione degli acquisti e delle terze parti* . I requisiti di sicurezza applicabili alle terze parti devono essere definiti contrattualmente a cura della funzione NDA\Contract Evaluation in collaborazione con il RSGSI.

Collegamento con la struttura organizzativa formale

La presente mappatura delle responsabilità è strettamente collegata ai documenti organizzativi dell'azienda. Il *MOD Organigramma* , approvato dal Chief Executive Officer, rappresenta la macrostruttura aziendale con le relative linee gerarchiche, suddivise in Business Functions, Support Functions e Line Functions. Il *MOD Mansionario* , gestito dalla funzione HR e approvato dal Top Management, descrive in dettaglio i compiti, le responsabilità e i requisiti minimi di competenza per ciascuna posizione.

I responsabili di ciascuna funzione aziendale devono assicurare che il personale sotto la propria responsabilità applichi la sicurezza delle informazioni in conformità con le politiche e le procedure dell'organizzazione, integrando i requisiti di sicurezza nelle attività e nei processi del proprio team. In caso di non conformità o violazioni, i responsabili

collaboreranno con la funzione HR e con il RSGSI per la gestione delle azioni correttive e disciplinari.

Archiviazione e aggiornamento

La presente politica è un documento controllato, archiviato e gestito in formato digitale secondo le disposizioni della *PRO Procedura di gestione delle informazioni documentate* . Il RSGSI è responsabile della sua custodia, distribuzione e aggiornamento.

La politica dev'essere riesaminata con cadenza almeno annuale, oppure a seguito di:

- Modifiche organizzative significative alla struttura aziendale, all'organigramma o al mansionario
- Esiti di audit interni o esterni che evidenzino necessità di adeguamento
- Cambiamenti nel contesto normativo, tecnologico o delle minacce
- Raccomandazioni emerse durante il riesame della direzione

Qualsiasi modifica alla presente politica dev'essere approvata dal Top Management, documentata con indicazione della versione e della data di revisione e comunicata a tutto il personale e alle parti interessate rilevanti.

Documenti di riferimento

- MOD Organigramma
- MOD Mansionario
- POL Politica di sicurezza delle informazioni
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- PRO Procedura di gestione delle risorse umane
- PRO Procedura di gestione degli acquisti e delle terze parti
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione e controllo degli accessi logici
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione del cambiamento
- PRO Gestione audit interni
- PRO Gestione riesame della direzione
- PRO Procedura dei ruoli e responsabilità
- Codice di condotta