POL Politica di classificazione ed etichettatura 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 istituire il framework aziendale per la classificazione e l'etichettatura di tutte le informazioni e degli asset informativi di DG Impianti Industriali S.p.A. Il documento stabilisce un sistema strutturato a tre livelli di criticità e sensibilità, fornendo per ciascuno esempi concreti tratti dal contesto operativo dell'organizzazione nei settori dell'energia, oil & gas, petrolchimico e farmaceutico. L'organizzazione classifica le informazioni in base ai requisiti legali applicabili, alla loro sensibilità e alla criticità per il business, al fine di garantire che a ogni asset venga applicato un livello di protezione adeguato e proporzionato al suo valore e al rischio associato. La politica definisce inoltre le modalità operative per l'etichettatura delle informazioni, rendendo la classificazione immediatamente visibile, e associa a ciascun livello specifici requisiti di protezione per il trattamento, la trasmissione e la conservazione dei dati.

Campo di applicazione

La presente politica si applica a tutte le informazioni e ai sistemi informativi di DG Impianti Industriali S.p.A., indipendentemente dal formato (digitale o cartaceo) e dal supporto su cui sono archiviate o trasmesse. Il suo ambito copre le sedi di Via Napo Torriani n.22, Milano, e di Via Antonio Vivaldi n.4, Montesilvano (PE), nonché qualsiasi ubicazione in cui il personale operi in modalità remota o in trasferta presso clienti.

La politica shall essere rispettata da tutto il personale dipendente, dai collaboratori a contratto e dalle terze parti autorizzate ad accedere alle informazioni aziendali. Ogni sistema informatico shall essere classificato in base al livello più elevato delle informazioni che memorizza o elabora.

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.
- **D.Lgs. 196/2003:** Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 101/2018.

Termini e definizioni

- **Classificazione delle informazioni:** Il processo di valutazione delle informazioni in base alla loro sensibilità, criticità e requisiti legali, al fine di assegnarle a una delle categorie di protezione definite dalla presente politica.
- **Etichettatura delle informazioni:** L'atto di apporre un'etichetta fisica o digitale a un'informazione per indicarne il livello di classificazione e facilitarne il corretto trattamento da parte di chiunque ne entri in possesso.

- **Proprietario delle informazioni:** La persona o la funzione aziendale che detiene la responsabilità principale per un determinato set di informazioni, inclusa l'assegnazione della classificazione e l'autorizzazione all'accesso.
- **Need-to-know:** Il principio in base al quale l'accesso alle informazioni è concesso esclusivamente ai soggetti che ne hanno una comprovata necessità lavorativa per lo svolgimento delle proprie mansioni.
- **Supporto di memorizzazione:** Qualsiasi dispositivo fisico o digitale utilizzato per archiviare informazioni, inclusi dischi rigidi, unità USB, CD/DVD, server e servizi cloud.

Ruoli e responsabilità

- **ICT-RSGSI:** Supervisiona l'implementazione e il rispetto della presente politica, gestisce le richieste di eccezione e le segnalazioni di violazione, e coordina le attività di riesame periodico dello schema di classificazione.
- **Chief Executive Officer:** Approva la presente politica e le eventuali modifiche sostanziali allo schema di classificazione, assicurando la disponibilità delle risorse necessarie per la sua attuazione.
- **Proprietari delle informazioni (tutti i responsabili di funzione):** Classificano le informazioni sotto il proprio controllo, ne riesaminano periodicamente la classificazione, approvano le richieste di accesso e identificano eventuali requisiti di protezione aggiuntivi.
- **Dipendenti, collaboratori e terze parti autorizzate:** Custodiscono in modo sicuro le informazioni sotto il proprio controllo e le trattano in conformità con la loro classificazione ed etichettatura, segnalando tempestivamente qualsiasi anomalia o violazione all'ICT-RSGSI.

Classificazione delle informazioni

DG Impianti Industriali S.p.A. adotta tre livelli di classificazione per garantire che ogni asset informativo riceva una protezione proporzionata alla sua sensibilità e al rischio associato. Ogni sistema informatico shall essere classificato in base al livello più elevato delle informazioni che memorizza o elabora. Il proprietario delle informazioni è responsabile dell'assegnazione iniziale della classificazione e del suo riesame periodico, con cadenza almeno annuale o a seguito di cambiamenti significativi nel contesto di utilizzo.

Riservato

Rientrano in questa categoria le informazioni altamente sensibili che richiedono il massimo livello di protezione. L'accesso è strettamente limitato a dipendenti o ruoli specifici e pre-autorizzati dal proprietario delle informazioni. La divulgazione non autorizzata di informazioni riservate può causare danni gravi all'organizzazione, ai suoi clienti o ai suoi partner, incluse conseguenze legali, finanziarie o reputazionali.

Esempi: informazioni di identificazione personale (PII) dei dipendenti e dei collaboratori, dati finanziari e bancari aziendali, informazioni su stipendi e compensi, piani strategici

aziendali, dati tecnici riservati di progetto relativi a commesse nei settori energia, oil & gas e farmaceutico, segreti commerciali, chiavi crittografiche, credenziali di autenticazione, *MOD Registro dei trattamenti del titolare* , anagrafiche utenti e inventario degli asset IT.

Limitato

Questa classe comprende le informazioni proprietarie dell'azienda che, pur non essendo sensibili come quelle riservate, richiedono una protezione adeguata per preservare gli interessi aziendali. L'accesso è limitato ai dipendenti e ai collaboratori che ne hanno una comprovata necessità lavorativa (need-to-know). **Questa è la classificazione predefinita per tutte le informazioni aziendali non diversamente classificate.** In assenza di un'esplicita attribuzione da parte del proprietario, ogni informazione aziendale shall essere trattata come Limitata.

Esempi: procedure interne e istruzioni operative del Sistema di Gestione, contratti con clienti e fornitori, verbali di riunioni, report interni di avanzamento progetto, documentazione tecnica e progettuale IT, la maggior parte delle comunicazioni email interne, *MOD Conservazione delle informazioni e degli asset* , *MOD Modulo di assegnazione dei beni* .

Pubblico

Include tutte le informazioni destinate alla diffusione pubblica e che possono essere distribuite liberamente al di fuori dell'organizzazione senza rischi per il business. La pubblicazione di informazioni con classificazione Pubblico shall comunque essere autorizzata dal proprietario delle informazioni o dalla funzione competente.

Esempi: materiale di marketing e comunicazione istituzionale, descrizioni di servizi e settori di attività, politiche aziendali destinate alla pubblicazione esterna, contenuti del sito web aziendale.

Etichettatura delle informazioni

L'etichettatura è il meccanismo attraverso cui la classificazione di un'informazione viene resa visibile, garantendone un trattamento corretto da parte di tutti gli utenti. Tutte le informazioni classificate come "Riservato" o "Limitato" shall essere etichettate secondo le modalità descritte di seguito. Le informazioni classificate come "Pubblico" non richiedono etichettatura obbligatoria, salvo diversa indicazione del proprietario delle informazioni.

- **Documenti elettronici:** I documenti shall riportare l'etichetta di classificazione (ad esempio "RISERVATO" o "LIMITATO") nell'intestazione, nel piè di pagina o come filigrana (watermark). I modelli aziendali predisposti dalla funzione Document Control già integrano il campo di classificazione; il proprietario del documento è tenuto a compilarlo prima della distribuzione.
- **Email:** Le email contenenti informazioni sensibili shall includere l'etichetta di classificazione nel campo oggetto, anteponendola al testo del soggetto (ad esempio " [RISERVATO] Oggetto del messaggio"). Per le email contenenti informazioni Limitate,

l'etichetta should essere apposta quando il messaggio è destinato a soggetti esterni all'organizzazione.

- **Supporti fisici:** I documenti cartacei classificati come Riservato o Limitato shall essere fisicamente contrassegnati con l'etichetta corrispondente in modo ben visibile sulla prima pagina. I supporti di memorizzazione rimovibili, come unità USB o dischi esterni, qualora il loro uso sia eccezionalmente autorizzato dall'ICT-RSGSI, shall riportare un'etichetta fisica ben visibile che ne indichi il livello di classificazione.
- **Sistemi e repository digitali:** Le cartelle di rete e i repository documentali su SharePoint shall riflettere la classificazione attraverso la denominazione o i metadati associati. L'accesso ai repository è gestito tramite Active Directory in base ai gruppi di appartenenza assegnati dagli amministratori, coerentemente con il livello di classificazione delle informazioni contenute.

Gestione delle informazioni

Trattamento delle informazioni

Il trattamento delle informazioni shall avvenire in stretta conformità con il loro livello di classificazione. La tabella seguente riassume i requisiti di protezione associati a ciascun livello.

Requisito	Riservato	Limitato	Pubblico
Controllo degli accessi	Accesso limitato, tracciato e nominativo; nessun accesso anonimo consentito. Autorizzazione esplicita del proprietario delle informazioni.	Accesso concesso sulla base del principio need-to-know; nessun accesso anonimo consentito.	Nessuna restrizione specifica di accesso.
Crittografia at-rest	Obbligatoria. I dischi dei laptop e dei dispositivi mobili shall essere crittografati. I backup shall essere crittografati.	Raccomandata per i supporti rimovibili e i dispositivi mobili.	Non richiesta.
Crittografia in-transit	Obbligatoria per qualsiasi trasmissione su reti pubbliche o esterne.	Obbligatoria per trasmissioni verso destinatari esterni all'organizzazione.	Non richiesta.

Protezione dei dispositivi	Blocco schermo automatico dopo 5 minuti di inattività, protetto da password o biometria. Divieto di archiviazione su dispositivi personali o supporti rimovibili non approvati.	Blocco schermo automatico secondo le policy centralizzate. Custodia sicura dei documenti cartacei.	Nessun requisito aggiuntivo.
Mascheramento dei dati	Shall essere applicato quando i dati riservati (incluse le PII) sono utilizzati in ambienti non di produzione o condivisi con soggetti non autorizzati all'accesso integrale, mediante tecniche di pseudonimizzazione, anonimizzazione o sostituzione.	Should essere valutato caso per caso in base alla natura dei dati.	Non applicabile.
Smaltimento	Cancellazione sicura certificata (software wipe multi-passaggio o distruzione fisica); lo smaltimento shall essere documentato in un verbale di cancellazione.	Cancellazione sicura dei supporti digitali; distruzione dei documenti cartacei tramite distruggi-documenti.	Smaltimento ordinario senza requisiti specifici.
Prevenzione della fuga di dati	Le policy DLP aziendali, implementate tramite la piattaforma Sophos Central, shall essere attive per monitorare e bloccare il trasferimento non	I controlli DLP should essere configurati per rilevare trasferimenti anomali di volumi significativi di dati.	Non applicabile.

	autorizzato di dati riservati verso supporti esterni, email, servizi di messaggistica e browser.		
Conservazione	Secondo i periodi definiti nel *MOD Conservazione delle informazioni e degli asset* . Al termine del periodo, cancellazione sicura obbligatoria.	Secondo i periodi definiti nel *MOD Conservazione delle informazioni e degli asset* . Al termine del periodo, cancellazione sicura.	Nessun periodo di conservazione obbligatorio specifico, salvo requisiti legali.
Protezione dei documenti	Le registrazioni shall essere protette da perdita, distruzione, falsificazione e accesso non autorizzato tramite controlli di accesso rigorosi, backup crittografati e segregazione dei diritti.	Le registrazioni shall essere protette tramite controlli di accesso basati sui ruoli e backup periodici.	Protezione dall'alterazione non autorizzata prima della pubblicazione.

Trasferimento delle informazioni

Il trasferimento di informazioni al di fuori dell'organizzazione è strettamente controllato e shall avvenire nel rispetto delle regole seguenti.

- Il trasferimento a terzi di informazioni **Riservate** è permesso solo in presenza di un accordo legale o contrattuale che vincoli il destinatario alla riservatezza, e con l'esplicita autorizzazione del Chief Executive Officer o del proprietario delle informazioni. Tutti i trasferimenti elettronici shall avvenire esclusivamente tramite canali crittografati e i dati shall essere protetti in conformità con la *PRO Procedura di crittografia e gestione delle chiavi crittografiche* .
- Il trasferimento di informazioni **Limitate** richiede l'approvazione del proprietario delle informazioni e la sottoscrizione di un accordo di riservatezza (NDA) da parte del destinatario esterno, valutato dalla funzione NDA\Contract Evaluation. I trasferimenti elettronici shall avvenire tramite canali crittografati.
- Le informazioni **Pubbliche** possono essere trasferite liberamente, a condizione che la loro pubblicazione sia stata preventivamente autorizzata dal proprietario delle informazioni o dalla funzione competente.

In ogni caso, il personale shall verificare la classificazione delle informazioni prima di procedere al trasferimento e shall accertarsi che il destinatario sia autorizzato a riceverle. Qualsiasi trasferimento di dati personali verso paesi terzi extra-UE shall rispettare le disposizioni del GDPR in materia di trasferimenti internazionali.

Archiviazione e aggiornamento

La presente politica è un documento controllato, archiviato e gestito in formato digitale nel sistema di gestione documentale aziendale in conformità con la *PRO Procedura di gestione delle informazioni documentate* . Il documento shall essere riesaminato con cadenza annuale, o a seguito di cambiamenti significativi nell'organizzazione, nella tecnologia o nel contesto delle minacce, sotto la supervisione dell'ICT-RSGSI. L'approvazione delle modifiche sostanziali spetta al Chief Executive Officer.

Documenti di riferimento

- *PRO Procedura di gestione delle informazioni documentate*
- *POL Politica di sicurezza delle informazioni*
- *POL Politica di sicurezza operativa*
- *POL Politica di conservazione e cancellazione delle informazioni*
- *PRO Procedura di crittografia e gestione delle chiavi crittografiche*
- *PRO Procedura di gestione e controllo degli accessi logici*
- *PRO Procedura di configurazione, gestione e smaltimento degli asset*
- MOD Conservazione delle informazioni e degli asset
- MOD Modulo di assegnazione dei beni
- MOD Registro dei trattamenti del titolare