

POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	30/04/2026	Carlo Sperduti	Claudio Patelli

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Impegno e obiettivi del sistema di gestione
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

Bowman S.r.l. riconosce nella sicurezza delle informazioni un elemento strategico inscindibile dalla propria missione di progettazione, sviluppo, erogazione e gestione di soluzioni software proprietarie per la gestione documentale e l'analisi dei dati. La presente politica esprime la volontà del **Top Manager - Direzione, Finanza e HR** di orientare l'intera organizzazione verso la protezione della riservatezza, dell'integrità e della disponibilità del patrimonio informativo aziendale e dei dati dei propri clienti B2B, in conformità alla norma ISO/IEC 27001:2022.

Attraverso questo documento, Bowman formalizza i propri principi guida, gli impegni verso le parti interessate e il quadro entro cui sono definiti gli obiettivi di sicurezza delle informazioni. La politica promuove una cultura fondata sui valori di rispetto, integrità e collaborazione, affinché ogni persona coinvolta nelle attività aziendali contribuisca attivamente alla tutela degli asset informativi. La direzione si impegna a rendere la presente politica disponibile come informazione documentata, a comunicarla a tutto il personale e a metterla a disposizione delle parti interessate, pubblicandola sul sito aziendale affinché sia liberamente consultabile.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi di Bowman S.r.l., inclusi i sistemi informatici e l'infrastruttura cloud impiegati per lo sviluppo, l'erogazione e la gestione delle piattaforme EXPANDA e ALGORILLA e dei relativi servizi di assistenza. Il perimetro comprende la sede legale di Via Libero Temolo 4, Milano, nonché qualsiasi luogo dal quale il personale operi in modalità remota, compresi gli spazi di co-working utilizzati occasionalmente. Sono destinatari della politica tutti i dipendenti, i collaboratori e le terze parti che accedano alle informazioni o ai sistemi aziendali, indipendentemente dalla loro ubicazione.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- GDPR
- D.Lgs. 196/2003
- D.Lgs. 101/2018

Termini e definizioni

- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI):** insieme di politiche, processi e controlli che un'organizzazione adotta per gestire in modo sistematico i rischi relativi alla sicurezza delle informazioni, al fine di preservarne la riservatezza, l'integrità e la disponibilità.

- **Sicurezza delle informazioni:** preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza:** proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità:** proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità:** proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Rischio:** effetto dell'incertezza sugli obiettivi.
- **Valutazione del rischio:** processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio:** processo volto a modificare il rischio, attraverso la selezione e l'attuazione di controlli appropriati.
- **Parte interessata:** persona od organizzazione che può influenzare, essere influenzata da, o percepirsi influenzata da una decisione o un'attività.
- **Miglioramento continuo:** attività ricorrente finalizzata ad accrescere le prestazioni del sistema di gestione.
- **Informazione documentata:** informazione che deve essere tenuta sotto controllo e mantenuta dall'organizzazione, incluso il supporto che la contiene.
- **Politica:** intenzioni e orientamento di un'organizzazione, formalmente espressi dalla sua alta direzione.

Ruoli e responsabilità

- **Top Manager - Direzione, Finanza e HR:** approva la presente politica e ne verifica la coerenza con gli indirizzi strategici aziendali, assicurando le risorse necessarie al mantenimento e al miglioramento del SGSI.
- **Responsabile del Sistema di Gestione:** redige e aggiorna la presente politica, ne coordina la comunicazione interna ed esterna e verifica periodicamente che i contenuti restino allineati al contesto organizzativo e normativo.
- **CTO:** fornisce gli orientamenti tecnici affinché le piattaforme software e l'infrastruttura cloud siano coerenti con i principi e gli obiettivi di sicurezza espressi nella politica.
- **Responsabile Sistemi IT:** contribuisce alla valutazione dei controlli tecnici di sicurezza e garantisce che l'infrastruttura IT supporti gli impegni assunti nella presente politica.
- **Responsabile Partnership:** assicura che gli accordi con partner e integratori esterni riflettano i requisiti di sicurezza delle informazioni stabiliti dalla politica.
- **Responsabile Vendite:** promuove presso i clienti il valore della sicurezza delle informazioni come elemento distintivo dell'offerta aziendale.
- **Team di Sviluppo:** applica i principi di sicurezza della politica nell'intero ciclo di vita dello sviluppo software.

- **Team di Application Maintenance:** opera nel rispetto dei principi di sicurezza della politica durante le attività di manutenzione e supporto delle piattaforme.
- **Team Vendite:** integra i principi della politica nelle relazioni commerciali e nelle fasi di pre-vendita e onboarding dei clienti.

Impegno e obiettivi del sistema di gestione

Impegno della Direzione

Bowman S.r.l. fonda ogni decisione in materia di sicurezza delle informazioni su una valutazione sistematica dei rischi che possono compromettere il proprio patrimonio informativo. La probabilità e l'impatto potenziale di ciascun rischio vengono analizzati attraverso una scala strutturata; i rischi che superano la soglia di tolleranza stabilita dalla direzione sono trattati con controlli proporzionati, secondo la metodologia descritta nella *PRO Procedura di gestione dei rischi*. Questo approccio consente di allocare le risorse in modo mirato, dando priorità alla protezione degli asset più critici per il business.

Il Top Manager - Direzione, Finanza e HR si impegna a:

- garantire che la politica di sicurezza delle informazioni e i relativi obiettivi siano coerenti con la direzione strategica dell'organizzazione, orientata alla progettazione e allo sviluppo di piattaforme software proprietarie per la gestione intelligente dei contenuti digitali e l'analisi dei dati;
- assicurare la disponibilità delle risorse finanziarie, umane e tecnologiche necessarie al funzionamento e al miglioramento del SGSI;
- promuovere a tutti i livelli organizzativi una cultura della sicurezza delle informazioni, fondata sui valori di rispetto, integrità e collaborazione;
- integrare i requisiti del SGSI nei processi operativi quotidiani, affinché la protezione delle informazioni non sia un'attività a sé stante ma parte integrante di ogni processo aziendale;
- comunicare a tutto il personale l'importanza di una gestione efficace della sicurezza, favorendo la consapevolezza e la responsabilità condivisa;
- sostenere ciascun ruolo aziendale nell'esercizio delle proprie responsabilità in materia di sicurezza delle informazioni;
- soddisfare i requisiti applicabili, siano essi di natura legale, regolamentare o contrattuale;
- perseguire il miglioramento continuo del SGSI attraverso il riesame periodico delle prestazioni, l'analisi degli incidenti e l'adeguamento dei controlli.

Principi fondamentali

Bowman riconosce nella responsabilità condivisa un pilastro della propria strategia di sicurezza: ogni dipendente, collaboratore o terza parte che accede ai sistemi aziendali è tenuto a proteggere le informazioni trattate e a segnalare tempestivamente qualsiasi evento anomalo attraverso il canale dedicato, con garanzia di protezione da ritorsioni.

L'organizzazione adotta un sistema di classificazione delle informazioni su tre livelli - Riservato, Limitato e Pubblico - ciascuno associato a specifici requisiti di trattamento, trasmissione e conservazione, descritti nella *POL Politica di classificazione ed etichettatura delle informazioni*. A supporto della protezione quotidiana, sono applicate pratiche di scrivania e schermo puliti, incluso il blocco automatico dei dispositivi dopo cinque minuti di inattività.

Obiettivi di sicurezza delle informazioni

La presente politica costituisce il quadro di riferimento per la definizione degli obiettivi di sicurezza delle informazioni. In coerenza con il contesto organizzativo, le esigenze delle parti interessate e il profilo di rischio, Bowman persegue i seguenti obiettivi:

- proteggere la riservatezza, l'integrità e la disponibilità delle informazioni, con particolare attenzione alla sicurezza delle soluzioni EXPANDA e ALGORILLA, installate e operanti negli ambienti dei clienti B2B, e alle informazioni dei clienti a cui Bowman possa accedere nelle attività di installazione e assistenza;
- mantenere e rafforzare la fiducia degli stakeholder mediante una gestione della sicurezza trasparente ed efficace;
- assicurare la conformità ai requisiti legali, regolamentari e contrattuali applicabili;
- gestire in modo sistematico e proporzionato i rischi per la sicurezza delle informazioni, riducendo le vulnerabilità e prevenendo gli incidenti;
- promuovere la consapevolezza e la competenza del personale in materia di sicurezza, garantendo che ogni dipendente completi la formazione prevista;
- migliorare continuamente il SGSI, attraverso il riesame periodico delle prestazioni, l'analisi degli incidenti e l'adeguamento dei controlli.

Il raggiungimento degli obiettivi è monitorato tramite indicatori di prestazione definiti nella *PRO Procedura delle misurazioni e del monitoraggio* e riesaminato periodicamente dalla direzione in sede di riesame, secondo quanto previsto dalla *PRO Gestione riesame della direzione*. Se il riesame evidenzia la necessità di ridefinire la politica o gli obiettivi, il **Responsabile del Sistema di Gestione** comunica le modifiche a tutto il personale conformemente alla *PRO Procedura gestione comunicazione*.

Comunicazione della politica

La presente politica è comunicata internamente a tutto il personale tramite i canali aziendali approvati, quali posta elettronica aziendale, intranet, SharePoint e piattaforma di messaggistica aziendale, ogniquale volta sia pubblicata o aggiornata. La comunicazione è accompagnata dalla raccolta di evidenze di avvenuta ricezione. Esternamente, la politica è resa disponibile alle parti interessate attraverso la pubblicazione sul sito aziendale, nel footer della pagina, affinché sia liberamente scaricabile e consultabile da chiunque vi acceda.

Archiviazione e aggiornamento

La presente politica è archiviata in formato elettronico sugli strumenti approvati dall'organizzazione, protetta da controlli di accesso logico proporzionati alla propria classificazione. Ogni versione approvata è sottoposta a controllo di versione, che registra autore, data e natura della modifica. Le versioni superate sono rimosse dal repository attivo per evitarne l'uso accidentale, ma restano accessibili su richiesta a fini di audit. Il **Responsabile del Sistema di Gestione** riesamina la politica almeno una volta all'anno, oppure a seguito di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, e propone gli aggiornamenti necessari al **Top Manager - Direzione, Finanza e HR**, che ne autorizza formalmente la pubblicazione. Ogni aggiornamento comporta l'incremento del numero di revisione e la registrazione della modifica nell'elenco della documentazione del SGSI.

Documenti di riferimento

- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura delle misurazioni e del monitoraggio
- PRO Gestione riesame della direzione
- PRO Procedura gestione comunicazione