					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P01S					Titolo del documento: **Politica per la sicurezza delle informazioni**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento, ove applicabile, a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.1, 5.2, 5.3, 6.1, 6.2, 8	Definisce l'impegno della direzione, i requisiti della politica, l'assegnazione dei ruoli, la valutazione del rischio e il controllo operativo
ISO/IEC 27002:2022	Controlli 5.1–5	Definisce la predisposizione di politiche documentate per la sicurezza delle informazioni, l'assegnazione dei ruoli, la segregazione dei compiti e le responsabilità della direzione
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Requisiti relativi al piano del programma di sicurezza, alla politica di pianificazione, alla valutazione/autorizzazione e al controllo degli accessi
GDPR UE (2016/679)	Articolo 5(2), Articolo 32	Principio di accountability e misure di sicurezza del trattamento, con particolare riferimento ai ruoli documentati
Direttiva UE NIS2 (2022/2555)	Articolo 21(2)(a)	Richiede misure di gestione del rischio, ruoli e responsabilità per il rischio cyber
Regolamento UE DORA (2022/2554)	Articolo 9, Articolo 10	Richiede l'assegnazione di ruoli per la gestione del rischio ICT e la continuità operativa
COBIT 2019	EDM03, APO13, DSS05	Garantisce l'ottimizzazione del rischio, la gestione della sicurezza e la gestione dei servizi di sicurezza mediante una chiara assegnazione dei ruoli

1. Scopo

1.1 La presente politica formalizza l'impegno dell'organizzazione nella protezione delle informazioni aziendali e dei clienti, definendo con chiarezza responsabilità e misure di sicurezza pratiche, adeguate anche a organizzazioni prive di un team IT dedicato.

1.2 Essa garantisce che tutti i dipendenti, i collaboratori esterni e i fornitori di servizi rispettino regole vincolanti, consentendo la piena conformità ai requisiti di certificazione ISO/IEC 27001.

1.3 La presente politica consente all'organizzazione di rafforzare la fiducia dei clienti, dimostrando in modo chiaro come le loro informazioni siano protette mediante responsabilità definite, processi strutturati e una chiara attribuzione delle responsabilità.

2. Ambito di applicazione

2.1 La presente politica si applica a tutti i soggetti che accedono ai dati e ai sistemi dell'organizzazione o li gestiscono, inclusi:

2.1.1 Titolari dell'attività e direttori generali

2.1.2 Dipendenti, collaboratori esterni e tirocinanti

2.1.3 Fornitori esterni di servizi IT o consulenti

2.2 Essa si applica a tutte le tipologie di informazioni, sistemi e servizi, inclusi:

2.2.1 Registrazioni aziendali, dati dei clienti, password ed e-mail

2.2.2 Dispositivi IT quali laptop e telefoni

2.2.3 Servizi cloud utilizzati per l'archiviazione di file, la comunicazione o le attività finanziarie

2.2.4 Documenti cartacei conservati presso le sedi aziendali

2.3 La politica si applica a tutti gli ambienti di lavoro — in ufficio, da remoto e in cloud — e comprende tutti i dispositivi e i software utilizzati per trattare o archiviare informazioni aziendali.

3. Obiettivi

3.1 Assegnare responsabilità chiare: garantire che vi sia sempre un soggetto responsabile della sicurezza delle informazioni. Di norma, tale ruolo è svolto dal Direttore generale (GM) o dalla persona da questi formalmente designata.

3.2 Proteggere le informazioni dei clienti e dell'organizzazione: adottare misure di sicurezza affidabili e coerenti per prevenire l'uso improprio, la perdita o il furto di dati sensibili, comprese le registrazioni dei clienti e quelle finanziarie.

3.3 Supportare la certificazione ISO/IEC 27001: consentire all'organizzazione di dimostrare la piena conformità ai requisiti della ISO/IEC 27001, assicurando la capacità di dimostrare la conformità in sede di audit e l'idoneità alla certificazione senza richiedere infrastrutture complesse.

3.4 Integrare la sicurezza nelle operazioni aziendali: integrare la sicurezza delle informazioni nelle attività e nelle decisioni quotidiane in tutta l'organizzazione.

3.5 Promuovere la consapevolezza e la cultura della sicurezza: assicurare che ogni dipendente comprenda e rispetti le pratiche di sicurezza, come l'uso di password robuste e la segnalazione di attività sospette.

4. Ruoli e responsabilità

4.1 Direttore generale o titolare dell'attività

4.1.1 Ha la piena responsabilità della sicurezza delle informazioni.

4.1.2 Approva e mantiene la presente politica.

4.1.3 Garantisce che tutte le attività chiave di sicurezza siano gestite direttamente oppure formalmente delegate per iscritto.

4.1.4 Verifica che ogni attività di sicurezza delegata, quali la gestione degli accessi degli utenti o la risposta agli incidenti, sia svolta efficacemente.

4.1.5 Funge da punto di contatto predefinito per tutte le questioni di sicurezza interne ed esterne, inclusi audit e richieste dei clienti.

4.1.6 Monitora, in sede di riesame annuale, i progressi rispetto a tali obiettivi. Gli obiettivi devono essere misurabili ove possibile (ad es. percentuale di personale formato, numero di incidenti segnalati, ecc.) e devono essere aggiornati sulla base delle risultanze di sicurezza e delle variazioni del rischio.

4.2 Dipendente designato (se applicabile)

4.2.1 Può supportare il Direttore generale nella gestione delle attività operative quotidiane, quali la creazione di account utente, la revoca degli accessi per il personale cessato o il coordinamento con il fornitore di supporto IT.

4.2.2 Deve essere formalmente designato e disporre di autorità e strumenti sufficienti per svolgere i compiti assegnati.

4.2.3 Riporta eventuali problematiche al Direttore generale.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1 Riesame annuale

9.1.1 La presente politica deve essere sottoposta a riesame dal Direttore generale (GM) almeno una volta all'anno per garantire la continua conformità ai requisiti di certificazione ISO/IEC 27001, alle modifiche legislative e regolamentari (quali GDPR, NIS2 e DORA) e all'evoluzione delle esigenze aziendali.

9.2 Riesami intermedi

9.2.1 Ulteriori riesami devono essere effettuati ogniqualvolta si verifichino cambiamenti significativi, quali:

9.2.1.1 Incidenti o violazioni di sicurezza rilevanti.

9.2.1.2 Introduzione di nuovi processi aziendali o tecnologie (ad es. nuovo software, piattaforme per il lavoro da remoto o servizi cloud).

9.2.1.3 Modifiche dei requisiti legali o regolamentari che incidono sulla gestione delle informazioni.

9.3 Documentazione delle modifiche

9.3.1 Tutti i riesami e le modifiche della politica devono essere formalmente documentati, indicando chiaramente la data, la natura delle revisioni e l'approvazione del GM.

9.3.2 Una registrazione storica delle versioni della politica deve essere mantenuta in modo sicuro per dimostrare l'evoluzione della politica e la conformità in sede di audit.

9.4 Comunicazione degli aggiornamenti

9.4.1 Qualsiasi modifica alla presente politica deve essere comunicata tempestivamente a tutti i dipendenti, ai collaboratori esterni e alle terze parti pertinenti.

9.4.2 Le versioni aggiornate della politica devono essere facilmente accessibili a tutto il personale interessato (ad es. condivise elettronicamente o affisse fisicamente sul luogo di lavoro).

10. Politiche correlate e collegamenti

10.1 La presente politica si integra strettamente con altre politiche del set SME dell'organizzazione, in particolare:

10.1.1 P2S – Politica su ruoli e responsabilità di governance: chiarisce l'assegnazione dei compiti e delle responsabilità in materia di sicurezza.

10.1.2 P4S – Politica di controllo degli accessi: definisce la gestione sicura dell'accesso alle informazioni aziendali.

10.1.3 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: fornisce linee guida essenziali per la formazione e la sensibilizzazione del personale.

10.1.4 P17S – Politica di protezione dei dati e privacy: garantisce la conformità al GDPR e alle altre normative in materia di protezione dei dati.

10.1.5 P30S – Politica di risposta agli incidenti: descrive in dettaglio le azioni richieste in risposta agli incidenti di sicurezza.

10.2 Tali politiche collegate forniscono indirizzi operativi chiari e devono essere applicate congiuntamente per conseguire la piena conformità ai fini della certificazione ISO/IEC 27001.

11. Norme e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 5.1 – Leadership e impegno: richiede l'impegno dell'alta direzione e la responsabilità in merito all'efficacia della sicurezza delle informazioni all'interno dell'organizzazione.

11.1.2 Clausola 5.2 – Politica per la sicurezza delle informazioni: richiede politiche chiare e documentate, allineate alla strategia organizzativa e ai requisiti di conformità.

11.1.3 Clausola 5.3 – Ruoli e responsabilità organizzativi: definisce una chiara assegnazione delle responsabilità per la sicurezza delle informazioni nell'intera organizzazione, essenziale per un'efficace governance e per la conformità in sede di audit.

11.1.4 Clausola 6.1 – Azioni per affrontare rischi e opportunità: garantisce che i rischi per la sicurezza delle informazioni siano identificati, valutati e trattati in modo sistematico.

11.1.5 Clausola 8.1 – Pianificazione e controllo operativi: richiede all'organizzazione di pianificare e attuare i processi necessari per conseguire gli obiettivi di sicurezza delle informazioni e gestire efficacemente i rischi associati.

11.2 Controlli 5.1–5 della ISO/IEC 27002:2022

11.2.1 Allegato A Controllo 5.1 – Politiche per la sicurezza delle informazioni: specifica la predisposizione e la comunicazione di politiche documentate per la sicurezza delle informazioni.

11.2.2 Allegato A Controllo 5.2 – Ruoli per la sicurezza delle informazioni: chiarisce e assegna formalmente ruoli e responsabilità per la sicurezza delle informazioni alle parti pertinenti.

11.2.3 Allegato A Controllo 5.3 – Segregazione dei compiti: impone una chiara separazione dei compiti per ridurre i conflitti di interesse e i rischi di frode nella gestione di informazioni sensibili.

11.2.4 Allegato A Controllo 5.4 – Responsabilità della direzione: richiede che la direzione dimostri il proprio impegno verso la sicurezza delle informazioni attraverso una supervisione attiva e l'allocazione delle risorse.

11.2.5 Rafforza la necessità di politiche, ruoli, responsabilità e strutture di governance per la sicurezza delle informazioni chiaramente documentati, assicurando una gestione coerente e la tracciabilità ai fini di audit in tutta l'organizzazione.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Piano del programma di sicurezza delle informazioni: richiede strategie e politiche documentate di governance della sicurezza delle informazioni, fornendo un quadro di riferimento per un'attuazione e una gestione coerenti.

11.3.2 PL-1 – Politica di pianificazione della sicurezza: richiede una politica di pianificazione della sicurezza estesa a tutta l'organizzazione per guidare il funzionamento sicuro e l'allineamento strategico delle attività di sicurezza delle informazioni.

11.3.3 CA-1 – Politica di valutazione e autorizzazione della sicurezza: richiede ruoli chiaramente definiti per la valutazione e l'autorizzazione, al fine di garantire efficacia continua e conformità ai requisiti di sicurezza delle informazioni.

11.3.4 AC-1 – Politica di controllo degli accessi: richiede alle organizzazioni di definire, documentare e applicare chiaramente le prassi e le responsabilità di gestione degli accessi.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 5(2) – Principio di accountability: richiede alle organizzazioni di dimostrare la conformità ai principi di protezione dei dati, inclusi ruoli e politiche documentati per le responsabilità in materia di protezione dei dati.

11.4.2 Articolo 32 – Sicurezza del trattamento: richiede l'attuazione di misure tecniche e organizzative adeguate, incluse chiare responsabilità di sicurezza, per proteggere i dati personali da violazioni e accessi non autorizzati.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(a) – Misure di gestione del rischio: richiede assetti di governance chiari, inclusi ruoli e responsabilità definiti per la sicurezza delle informazioni, essenziali per gestire efficacemente i rischi cyber.

11.6 Regolamento UE DORA (2022/2554)

11.6.1 Articolo 9 – Gestione del rischio ICT: richiede alle organizzazioni di assegnare chiaramente ruoli e responsabilità relativi alla gestione del rischio ICT, rafforzando la resilienza e la preparazione alla continuità operativa.

11.6.2 Articolo 10 – Continuità operativa ICT: richiede una chiara attribuzione delle responsabilità e ruoli strutturati per il mantenimento della resilienza e della continuità ICT, assicurando che le organizzazioni possano rispondere in modo affidabile alle interruzioni.

11.7 COBIT 2019

11.7.1 EDM03 – Garantire l'ottimizzazione del rischio: pone l'accento su responsabilità e ruoli chiaramente definiti nella gestione dei rischi dell'organizzazione, assicurando una governance solida e un'efficace supervisione dei rischi per la sicurezza delle informazioni.

11.7.2 APO13 – Gestire la sicurezza: richiede alle organizzazioni di definire e comunicare chiaramente le responsabilità per la gestione della sicurezza, assicurando l'allineamento con gli obiettivi aziendali e i requisiti normativi.

11.7.3 DSS05 – Gestire i servizi di sicurezza: richiede ruoli strutturati e responsabilità chiare nella gestione dei servizi di sicurezza, consentendo un'attuazione coerente e la verifica della conformità.