					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P08S					Titolo del documento: **Politica di consapevolezza e formazione sulla 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**

Allineata a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 7	
ISO/IEC 27002:2022	Controllo 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
Direttiva UE NIS2	Articolo 21(2)(i)	
Regolamento UE DORA	Articolo 13	
COBIT 2019	BAI08, DSS05	
GDPR UE	Articolo 32, 39	

1. Scopo

1.1. La presente politica garantisce che tutti i dipendenti e i collaboratori esterni comprendano le proprie responsabilità in materia di sicurezza delle informazioni.

1.2. Ha l'obiettivo di ridurre la probabilità di errore umano, migliorare la capacità di rilevare e segnalare gli incidenti e promuovere una cultura della sicurezza in tutta l'organizzazione.

1.3. La politica supporta la conformità a ISO/IEC 27001, NIS2, GDPR e DORA, integrando la consapevolezza della sicurezza nei comportamenti lavorativi quotidiani e nelle aspettative definite in base ai ruoli.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti i dipendenti, collaboratori esterni, tirocinanti e terze parti che hanno accesso ai sistemi o ai dati aziendali.

2.2. Include:

2.2.1. Formazione di sensibilizzazione alla sicurezza in fase di onboarding per il nuovo personale

2.2.2. Formazione annuale di aggiornamento e sensibilizzazione alla sicurezza

2.2.3. Attività di sensibilizzazione ad hoc (ad esempio aggiornamenti relativi agli incidenti, poster o consigli pratici)

2.3. Si applica a tutti i ruoli aziendali, a tutte le funzioni e a tutte le sedi.

3. Obiettivi

3.1. Garantire che tutto il personale riceva tempestivamente una formazione e sensibilizzazione sulla sicurezza delle informazioni comprensibile e pertinente.

3.2. Fornire ai dipendenti la capacità di identificare ed evitare minacce comuni quali phishing, malware e perdita di dati.

3.3. Stabilire evidenze documentali del completamento della formazione per dimostrare la conformità ai requisiti legali, contrattuali e di audit.

3.4. Mantenere contenuti formativi aggiornati che riflettano le politiche, le minacce e i requisiti normativi applicabili dell'organizzazione.

3.5. Promuovere nel personale un approccio proattivo, in cui la sicurezza sia considerata parte delle responsabilità quotidiane.

4. Ruoli e responsabilità

4.1. Direttore Generale (GM)

4.1.1. Approva i requisiti formativi e garantisce l'allocazione delle risorse necessarie.

4.1.2. Riesamina i report di completamento ed effettua l'escalation dei casi di non conformità, ove necessario.

4.2. Office Manager / Risorse Umane (HR)

4.2.1. Coordina l'erogazione della formazione per i nuovi assunti e degli aggiornamenti annuali.

4.2.2. Mantiene le registrazioni della formazione e i log di completamento.

4.2.3. Garantisce la presa visione da parte del personale delle principali politiche di sicurezza e degli accordi di riservatezza.

[... 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 riesaminata annualmente dal Direttore Generale (GM) e dalle Risorse Umane (HR) per garantire che rifletta i rischi attuali, i requisiti normativi e le esigenze del personale.

9.2. Aggiornamenti intermedi

9.2.1. La politica e i contenuti formativi devono inoltre essere riesaminati e aggiornati a seguito di:

9.2.1.1. Un incidente di sicurezza significativo

9.2.1.2. Cambiamenti legali o contrattuali

9.2.1.3. Riorganizzazioni aziendali o migrazioni di sistema

9.3. Controllo delle versioni e distribuzione

9.3.1. Ogni aggiornamento deve includere:

9.3.1.1. Numero di versione e data di entrata in vigore

9.3.1.2. Sintesi delle modifiche

9.3.1.3. Approvazione del Direttore Generale (GM)

9.3.1.4. Archivio di tutte le versioni precedenti conservato per almeno tre anni

9.4. Comunicazione ai dipendenti

9.4.1. Gli aggiornamenti della politica devono essere comunicati a tutto il personale e, in caso di modifiche sostanziali, deve essere acquisita la presa visione.

10. Politiche correlate e collegamenti

10.1. La presente politica supporta quanto segue:

10.1.1. P2S – Politica sui ruoli e sulle responsabilità di governance: assegna la responsabilità del coordinamento e della supervisione della formazione

10.1.2. P3S – Politica sull'uso accettabile: rafforza le aspettative comportamentali trattate nella formazione

10.1.3. P4S – Politica di controllo degli accessi: garantisce che gli utenti comprendano l'importanza della sicurezza degli accessi

10.1.4. P7S – Politica di onboarding e cessazione del personale: integra la formazione nel processo di inserimento

10.1.5. P30S – Politica di risposta agli incidenti: garantisce che il personale sappia come segnalare gli incidenti tempestivamente e correttamente

11. Norme e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 7.3 – Richiede che le organizzazioni garantiscano che il personale sia consapevole delle proprie responsabilità e degli impatti sulla sicurezza

11.2. ISO/IEC 27002

11.2.1. Controllo 6.3 – Definisce le aspettative relative all'ambito e all'erogazione della formazione sulla sicurezza

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Richiede formazione di sensibilizzazione per gli utenti con accesso ai sistemi

11.3.2. AT-4 – Copre la formazione basata sui ruoli e le conseguenze della non conformità

11.4. GDPR UE

11.4.1. Articolo 32 – Richiede misure di sicurezza, inclusa la formazione del personale, per proteggere i dati personali

11.4.2. Articolo 39 – Richiede che il DPO supervisioni le attività di sensibilizzazione e formazione, ove applicabile

11.5. Direttiva UE NIS2

11.5.1. Articolo 21(2)(i) – Richiede programmi continuativi di consapevolezza e formazione sulla cibersicurezza

11.6. Regolamento UE DORA

11.6.1. Articolo 13 – Richiede che le entità finanziarie attuino programmi di istruzione e formazione per tutto il personale con responsabilità relative ai sistemi ICT

11.7. COBIT 2019

11.7.1. BAI08 – Gestire la conoscenza: garantisce che il personale sia competente e adeguatamente formato

11.7.2. DSS05 – Gestire i servizi di sicurezza: evidenzia la sensibilizzazione come controllo chiave di protezione