					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P08					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 standard e normative

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 7.3, Annex A Control 6.3	Stabilisce i requisiti di consapevolezza e formazione disciplinati dalla presente politica
ISO/IEC 27002:2022	Control 6	Supporta una formazione di consapevolezza adeguata e basata sui ruoli
NIST SP 800-53 Rev.5	AT-1 to AT-5	Allineato con politiche e procedure, formazione di consapevolezza, formazione basata sui ruoli, registrazioni della formazione e contatto con i gruppi di sicurezza
EU GDPR	Articles 32, 39; Recital 78	Richiede la formazione del personale autorizzato al trattamento dei dati personali e la sensibilizzazione generale del personale
EU NIS2	Articles 21(2)(a, b), 21(3)	Richiede politiche di formazione su rischio e sicurezza e iniziative di sensibilizzazione
EU DORA	Articles 5, 8, 13	Richiede consapevolezza e formazione sul rischio ICT nell'ambito dei controlli di resilienza
COBIT 2019	APO07, DSS05, MEA	Rafforza la sensibilizzazione del personale, la formazione degli utenti e il monitoraggio della conformità

1. Finalità

1.1 La presente politica definisce il quadro formale per garantire che tutto il personale sia consapevole delle proprie responsabilità in materia di sicurezza delle informazioni e riceva la formazione necessaria a proteggere la riservatezza, l'integrità e la disponibilità (CIA) degli asset informativi.

1.2 Supporta la Clause 7.3 e l'Annex A Control 6.3 della ISO/IEC 27001, richiedendo un programma strutturato di consapevolezza e formazione, basato sul rischio e adattato ai ruoli organizzativi e all'evoluzione delle minacce.

1.3 La politica contribuisce a ridurre le vulnerabilità connesse al fattore umano, a promuovere comportamenti orientati alla sicurezza e a rafforzare in modo continuativo le pratiche sicure, in linea con i requisiti normativi e contrattuali.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le persone interne ed esterne che hanno accesso ai sistemi informativi, ai dati o alle strutture dell'organizzazione, inclusi:

2.1.1 dipendenti (a tempo pieno, part-time e personale temporaneo)

2.1.2 collaboratori esterni, consulenti, fornitori e tirocinanti

2.1.3 terze parti con accesso logico o fisico in base ad accordi di servizio

2.2 L'ambito di applicazione include:

2.2.1 formazione di consapevolezza sulla sicurezza in fase di onboarding

2.2.2 formazione specifica per ruolo (ad es. sviluppatori, personale dell'area finanza, utenti privilegiati)

2.2.3 aggiornamenti periodici e campagne di sensibilizzazione

2.2.4 formazione ad hoc in risposta a incidenti o nuove minacce

2.3 I metodi di erogazione della formazione coperti dalla presente politica includono e-learning, briefing in presenza, simulazioni, test di verifica delle conoscenze, poster, newsletter sulla sicurezza e prese d'atto obbligatorie.

3. Obiettivi

3.1 Garantire che tutto il personale comprenda le proprie responsabilità nella protezione degli asset dell'organizzazione e nel rispetto delle politiche di sicurezza.

3.2 Fornire una formazione continua e misurabile, allineata all'esposizione al rischio in funzione del ruolo.

3.3 Integrare comportamenti sicuri nelle attività quotidiane, rafforzando pratiche quali l'uso sicuro delle password, la segnalazione degli incidenti e la resistenza al phishing.

3.4 Garantire la conformità normativa e la capacità di dimostrarla ai fini di audit rispetto agli obblighi di formazione sulla sicurezza delle informazioni nei diversi settori e ordinamenti.

3.5 Ridurre gli incidenti di sicurezza derivanti da negligenza, scarsa consapevolezza o errori di valutazione attraverso il condizionamento comportamentale e il rafforzamento continuo.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva la strategia di formazione sulla sicurezza delle informazioni dell'organizzazione e assicura la disponibilità delle risorse necessarie, nonché l'integrazione di tale strategia nelle priorità aziendali.

4.1.2 Monitora la conformità a livello direzionale e assicura il rispetto della politica in tutti i dipartimenti.

4.2 Responsabile della sicurezza delle informazioni (CISO) / Responsabile del SGSI

4.2.1 È il titolare della presente politica e definisce il quadro di riferimento per la consapevolezza e la formazione in linea con rischio, conformità ed esigenze aziendali.

4.2.2 Sovrintende alla progettazione, all'erogazione, al tracciamento e al riesame di tutte le iniziative di formazione sulla sicurezza.

4.2.3 Garantisce che la formazione sia aggiornata periodicamente e rifletta l'evoluzione delle minacce e delle tecnologie emergenti.

[... 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 Frequenza di riesame

9.1.1 La presente politica e il relativo programma di formazione devono essere riesaminati:

9.1.1.1 annualmente, oppure

9.1.1.2 dopo incidenti rilevanti che coinvolgono errore umano o minacce interne

9.1.1.3 in occasione dell'introduzione di nuove tecnologie o minacce significative

9.1.1.4 in risposta a cambiamenti degli obblighi legali, contrattuali o di certificazione

9.2 Processo di riesame

9.2.1 Il riesame deve essere condotto dal CISO in coordinamento con:

9.2.1.1 i dipartimenti HR e formazione

9.2.1.2 la funzione legale e i responsabili della protezione dei dati (DPO)

9.2.1.3 le funzioni di sicurezza IT e rischio operativo

9.2.2 Tutti gli aggiornamenti devono essere:

9.2.2.1 approvati dal Comitato direttivo del SGSI

9.2.2.2 soggetti a controllo di versione e documentati nel registro documentale del SGSI

9.2.2.3 comunicati agli utenti se le modifiche sostanziali incidono sull'ambito o sulle responsabilità della formazione

9.3 Governance dell'aggiornamento dei contenuti

9.3.1 I moduli formativi e i materiali di sensibilizzazione devono essere riesaminati ogni 12 mesi per garantire:

9.3.1.1 rilevanza rispetto al panorama delle minacce

9.3.1.2 accuratezza normativa

9.3.1.3 compatibilità di formato (ad es. accessibilità, localizzazione)

9.3.2 I contenuti obsoleti o fuorvianti devono essere ritirati immediatamente e sostituiti con alternative approvate.

10. Politiche correlate e collegamenti

10.1 La presente politica è supportata dalle seguenti politiche e ne supporta l'applicazione:

10.1.1 P01 – Politica per la sicurezza delle informazioni: stabilisce la consapevolezza della sicurezza come controllo fondamentale nel SGSI dell'organizzazione.

10.1.2 P03 – Politica di uso accettabile: richiede la presa d'atto dell'utente durante la formazione e chiarisce le responsabilità connesse all'uso quotidiano della tecnologia.

10.1.3 P07 – Politica di onboarding e cessazione del personale: assicura che la formazione sia integrata all'ingresso e tracciata per tutta la durata del rapporto di lavoro.

10.1.4 P06 – Politica di gestione del rischio: collega la formazione incentrata sul fattore umano alla modellazione delle minacce e alle strategie di riduzione del rischio residuo.

10.1.5 P33 – Politica di monitoraggio dell'audit e della conformità: verifica che i controlli di sensibilizzazione siano operativi, misurabili ed efficaci durante gli audit.

10.2 Nel loro insieme, queste politiche costituiscono un quadro completo di controlli comportamentali che integra consapevolezza, responsabilizzazione e rafforzamento culturale.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clause 7.3 – Awareness: richiede alle organizzazioni di garantire che i lavoratori siano consapevoli delle politiche di sicurezza delle informazioni e delle proprie responsabilità. La presente politica rende operativo tale requisito tramite onboarding strutturato, formazione periodica e partecipazione misurabile alle campagne.

11.1.2 Annex A Control 6.3 – Formazione e consapevolezza sulla sicurezza delle informazioni: pienamente soddisfatto tramite programmi di formazione iniziale, basati sui ruoli e continuativi, adattati ai profili di rischio degli utenti.

11.2 ISO/IEC 27002:2022 – Control 6

11.2.1 Supporta lo sviluppo e l'erogazione di formazione di consapevolezza appropriata ai ruoli, con enfasi sul rafforzamento dei comportamenti sicuri e su aggiornamenti periodici basati sulle informazioni sulle minacce e sul feedback degli audit.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 to AT-5 (famiglia Awareness and Training): la presente politica è allineata ad AT-1 (Policy and Procedures), AT-2 (Awareness Training), AT-3 (Role-Based Training), AT-4 (Security Training Records) e AT-5 (Contact with Security Groups).

11.3.2 IA-5, AC-2: rafforza la responsabilità dell'utente in materia di autenticazione sicura e uso accettabile, aspetti centrali per gli esiti comportamentali dei programmi di sensibilizzazione.

11.3.3 IR-1 through IR-8: la preparazione alla risposta agli incidenti è rafforzata tramite campagne di sensibilizzazione mirate e simulazioni.

11.4 GDPR UE (2016/679)

11.4.1 Article 32 – Sicurezza del trattamento: richiede che il personale che tratta dati personali sia formato per riconoscere, prevenire e segnalare i rischi per i dati personali. La presente politica assicura che il personale autorizzato al trattamento dei dati personali e tutti i ruoli pertinenti ricevano una formazione adeguata.

11.4.2 Article 39 – Compiti del Responsabile della protezione dei dati (DPO): include la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento.

11.4.3 Recital 78: incoraggia misure di sensibilizzazione adeguate per garantire pratiche di sicurezza solide e conformità alle politiche.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Article 21(2)(a, b): richiede che i soggetti adottino politiche sull'analisi del rischio e sulla formazione in materia di sicurezza per tutto il personale rilevante. La presente politica soddisfa tale requisito istituendo processi di formazione continui e calibrati sul ruolo.

11.5.2 Article 21(3): incoraggia la promozione della consapevolezza del rischio di cibersicurezza tra management e personale attraverso iniziative di sensibilizzazione e simulazioni.

11.6 DORA UE (2022/2554)

11.6.1 Article 13 – Strategia di resilienza operativa digitale: richiede che la consapevolezza e la formazione sul rischio ICT facciano parte del modello di governance. La presente politica assicura che il rischio umano sia gestito tramite formazione continua e simulazione delle minacce.

11.6.2 Articles 5 and 8: sottolineano l'importanza dei quadri di controllo interni, di cui la sensibilizzazione e la formazione costituiscono componenti fondamentali per la resilienza ICT e l'igiene informatica.

11.7 COBIT 2019

11.7.1 APO07 Gestire le risorse umane: rafforza la necessità di sviluppare la consapevolezza delle responsabilità di sicurezza e di integrarla nella gestione del personale.

11.7.2 DSS05: stabilisce controlli sulla formazione degli utenti e sulla segnalazione degli incidenti, entrambi elementi integranti della presente politica.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: richiede il riesame dell'efficacia del comportamento degli utenti e della conformità alle politiche, qui attuato tramite test di phishing, quiz e metriche delle campagne di sensibilizzazione.