					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P25S					Titolo del documento: **Politica dei requisiti di sicurezza delle applicazioni**							
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 a standard e normative

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Controlli operativi, inclusa la sicurezza delle applicazioni
ISO/IEC 27002:2022	Controlli 8.25–8.26	Progettazione sicura, sviluppo, test e revisione del codice
NIST SP 800-53 Rev.5	SA-11, SI-10	Test degli sviluppatori e delle applicazioni, analisi del codice, prevenzione dei difetti
GDPR UE	Articolo 25	Protezione dei dati fin dalla progettazione e per impostazione predefinita
NIS2 UE	Articolo 21(2)(a), (e)	Misure tecniche per proteggere le applicazioni e rilevare i rischi
DORA UE	Articoli 9(2)(c), 10(2)(c)	Sicurezza delle applicazioni a supporto della resilienza operativa digitale
COBIT 2019	BAI03	Gestione dell'identificazione e dello sviluppo o acquisizione di software sicuro

1. Finalità

1.1 La presente politica definisce i controlli minimi obbligatori di sicurezza delle applicazioni richiesti per tutte le soluzioni software e di sistema utilizzate dall'organizzazione, indipendentemente dal fatto che siano sviluppate internamente o acquisite da fornitori esterni.

1.2 La politica garantisce che le applicazioni siano progettate, implementate e mantenute in modo da proteggere i dati di clienti, dipendenti e aziendali da accessi non autorizzati, uso improprio, alterazione o distruzione.

1.3 La presente politica supporta l'organizzazione nel conseguimento e nel mantenimento della certificazione ISO/IEC 27001, nell'adempimento degli obblighi derivanti da GDPR e NIS2 e nella riduzione dei rischi operativi associati a rilasci software non sicuri.

1.4 La politica contribuisce a creare un approccio coerente e verificabile alla sicurezza delle applicazioni per le piccole e medie imprese (PMI), definendo una checklist uniforme di funzionalità e pratiche di sicurezza, adattata ad ambienti con risorse tecniche interne limitate.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le applicazioni, ai sistemi, agli strumenti e alle piattaforme che:

2.1.1 Sono sviluppati internamente, personalizzati o realizzati tramite script per uso interno

2.1.2 Sono acquistati come software commerciale, SaaS o sistemi basati su cloud

2.1.3 Trattano, archiviano o trasmettono dati personali, registrazioni aziendali o informazioni operative sensibili

2.1.4 Sono accessibili da dipendenti, collaboratori esterni, clienti o partner tramite reti interne, Internet o piattaforme mobili

2.2 La politica si applica a:

2.2.1 Sviluppatori (interni o incaricati esternamente)

2.2.2 Fornitori di software e provider di servizi cloud

2.2.3 Personale di supporto IT o amministratori responsabili del rilascio e del supporto

2.2.4 Proprietari delle applicazioni e utenti aziendali coinvolti nell'approvazione e nella supervisione dei sistemi

3. Obiettivi

3.1 Garantire che tutte le applicazioni utilizzate dall'organizzazione dispongano di controlli di sicurezza integrati e verificabili che mitigano le vulnerabilità software comuni.

3.2 Proteggere la riservatezza, l'integrità e la disponibilità (CIA) dei dati trattati dalle applicazioni, indipendentemente da dove siano ospitate.

3.3 Richiedere test formali, riesame e convalida della sicurezza delle applicazioni prima che qualsiasi nuova applicazione o aggiornamento rilevante sia approvato per l'uso in produzione.

3.4 Consentire una gestione coerente e sicura delle credenziali utente, dei dati di sessione e dei diritti di accesso in tutti i sistemi critici per l'attività.

3.5 Richiedere funzionalità sicure di logging, tracciabilità e monitoraggio in tutte le applicazioni, a supporto del rilevamento e della risposta ad attività sospette.

3.6 Ridurre i rischi legali e di conformità garantendo che le applicazioni soddisfino i requisiti normativi di sicurezza applicabili.

4. Ruoli e responsabilità

4.1 Direttore Generale (GM)

4.1.1 Ha la responsabilità complessiva della sicurezza delle applicazioni nell'intera organizzazione.

4.1.2 Approva la presente politica e garantisce che tutte le acquisizioni o i progetti di sviluppo siano conformi ad essa.

4.1.3 Garantisce che fornitori e prestatori di servizi siano vincolati contrattualmente al rispetto dei requisiti di sicurezza delle applicazioni.

4.1.4 Riesamina e approva le eccezioni al rischio nei casi in cui la piena conformità non possa essere raggiunta per vincoli aziendali.

4.2 Proprietario dell'applicazione (ove designato)

4.2.1 Identifica le esigenze di sicurezza specifiche dell'applicazione durante la selezione del sistema o l'avvio del progetto.

4.2.2 Verifica che siano incluse funzionalità chiave quali protezione degli accessi, cifratura e registrazione delle attività.

4.2.3 Partecipa ai riesami pre-rilascio e conferma che i controlli di sicurezza soddisfino le esigenze aziendali.

[... 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 La presente politica deve essere riesaminata dal Direttore Generale almeno una volta per anno solare al fine di:

9.1.1 Riflettere le modifiche dei requisiti normativi (ad es. GDPR, NIS2, DORA)

9.1.2 Incorporare minacce e tecniche di attacco nuove o emergenti

9.1.3 Aggiornare il testo e i requisiti per riflettere i cambiamenti di piattaforme, fornitori o metodi di sviluppo

9.2 Devono inoltre essere effettuati riesami intermedi quando:

9.2.1 Vengono introdotte nuove applicazioni

9.2.2 Le applicazioni esistenti subiscono aggiornamenti significativi o integrazioni

9.2.3 Si verifica un incidente o una violazione correlata a un'applicazione

9.2.4 Vengono identificati nuovi rischi a seguito di avvisi esterni o allerte di settore

9.3 Tutti gli aggiornamenti alla presente politica devono essere:

9.3.1 Approvati dal Direttore Generale

9.3.2 Documentati con cronologia delle versioni e motivazione della modifica

9.3.3 Comunicati a tutti i dipendenti, sviluppatori e fornitori coinvolti nella gestione delle applicazioni

9.3.4 Archiviati in modo sicuro ai fini di audit e conformità

10. Politiche correlate e collegamenti

10.1 La presente politica è direttamente supportata dalle seguenti politiche di sicurezza allineate alle PMI e contribuisce alla loro applicazione:

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: assegna la responsabilità per l'approvazione delle applicazioni, l'applicazione della politica e la gestione dei fornitori.

10.1.2 P4S – Politica di controllo degli accessi: garantisce che l'accesso alle applicazioni sia allineato ai principi del privilegio minimo e del controllo delle sessioni.

10.1.3 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: garantisce che utenti e sviluppatori siano formati a riconoscere e segnalare minacce connesse alle applicazioni.

10.1.4 P17S – Politica di protezione dei dati e privacy: definisce le misure di tutela dei dati personali che devono essere applicate da qualsiasi applicazione che tratti informazioni personali.

10.1.5 P14S – Politica di conservazione e smaltimento dei dati: disciplina le modalità con cui i log generati dalle applicazioni, i backup e i dati sensibili devono essere conservati, archiviati e distrutti in modo sicuro.

10.1.6 P30S – Politica di risposta agli incidenti: definisce le fasi per identificare, segnalare e contenere eventi di sicurezza correlati alle applicazioni.

10.2 Nel loro insieme, tali politiche garantiscono che la sicurezza delle applicazioni sia pienamente integrata nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI) dell'organizzazione e che sia pronta ai fini di audit.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede alle organizzazioni di stabilire controlli operativi per affrontare i rischi per la sicurezza delle informazioni, inclusi quelli relativi ad applicazioni e sistemi software.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.25 – Raccomanda l'applicazione di pratiche di progettazione sicura, sviluppo sicuro e revisione del codice per tutte le applicazioni, comprese quelle fornite da vendor.

11.2.2 Controllo 8.26 – Raccomanda test formali dei controlli di sicurezza delle applicazioni, in particolare nelle aree del controllo degli accessi, della validazione degli input e della gestione delle sessioni.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Specifica requisiti per i test degli sviluppatori, l'analisi del codice e la scansione dinamica delle applicazioni prima del rilascio.

11.3.2 SI-10 – Riguarda il rilevamento e la prevenzione dei difetti software comuni, con enfasi sulla consapevolezza degli sviluppatori e sulle misure di sicurezza tecniche.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 25 – La “protezione dei dati fin dalla progettazione e per impostazione predefinita” impone di integrare privacy e sicurezza nella progettazione di base delle applicazioni che trattano dati personali.

11.5 Direttiva NIS2 UE (2022/2555)

11.5.1 Articolo 21(2)(a) e (e) – Richiede ai soggetti essenziali e importanti di implementare misure tecniche per proteggere le applicazioni e rilevare i rischi connessi al software.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 9(2)(c), 10(2)(c) – Richiede alle PMI del settore finanziario di integrare controlli di sicurezza a livello applicativo e di svolgere valutazioni regolari per mantenere la resilienza operativa digitale.

11.7 COBIT 2019

11.7.1 BAI03 – “Gestione dell'identificazione e dello sviluppo delle soluzioni” guida lo sviluppo o l'acquisizione di software sicuro, allineato a rischio, conformità e requisiti aziendali, anche in ambienti PMI con risorse limitate.