					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P24S					Titolo del documento: **Politica di sviluppo sicuro**							
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

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	Controlli di sicurezza pertinenti per le attività operative, incluso lo sviluppo sicuro
ISO/IEC 27002:2022	Controls 8.25–8.27	Copre il ciclo di vita dello sviluppo sicuro, i test e le responsabilità di sicurezza degli sviluppatori terzi
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Disciplina il ciclo di vita dello sviluppo sicuro, il controllo degli accessi e la gestione delle vulnerabilità nello sviluppo
GDPR UE	Article 25	Richiede la protezione dei dati fin dalla progettazione e per impostazione predefinita nello sviluppo software
NIS2 UE	Article 21(2)(a), (e), (h)	Impone politiche di sviluppo sicuro, supervisione sull'uso di componenti open source e documentazione delle misure di mitigazione
DORA UE	Articles 6(7), 9(1)(c), 10(2)(c)	Sicurezza del ciclo di vita per i sistemi ICT critici nel settore finanziario
COBIT 2019	BAI	Quadro di riferimento per una gestione dello sviluppo sicuro strutturata, tracciabile e resiliente

1. Finalità

1.1 La presente politica garantisce che tutto il software, gli script e gli strumenti web creati o modificati dall'organizzazione o dai suoi partner esterni siano sviluppati in modo sicuro, riducendo al minimo il rischio di vulnerabilità, accessi non autorizzati ai dati o interruzioni operative.

1.2 Definisce regole obbligatorie di sviluppo sicuro e pratiche di programmazione sicura che tutti gli sviluppatori interni, i collaboratori esterni e i fornitori devono seguire, indipendentemente dalle dimensioni o dalla complessità del progetto.

1.3 La presente politica è finalizzata a proteggere i dati dei clienti, prevenire violazioni dei dati e garantire che il software creato o personalizzato dall'organizzazione o per conto della stessa possa superare gli audit di sicurezza, soddisfare i requisiti legali (ad es. GDPR, NIS2, DORA) e supportare la certificazione ISO/IEC 27001.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le persone e a tutti i soggetti coinvolti nello sviluppo, nella personalizzazione, nel rilascio o nella gestione dei seguenti elementi per conto dell'organizzazione:

2.1.1 Siti web, applicazioni o strumenti di automazione

2.1.2 Script o software sviluppati internamente

2.1.3 Codice creato da sviluppatori terzi o freelance

2.1.4 Plugin, librerie e componenti software integrati nei sistemi in esercizio

2.2 Copre tutti gli ambienti utilizzati nelle attività di sviluppo, inclusi:

2.2.1 Ambienti di sviluppo e di test

2.2.2 Ambienti di staging e pre-produzione

2.2.3 Sistemi di produzione utilizzati per eseguire codice sviluppato su misura

2.3 La politica disciplina inoltre il trattamento dei dati durante lo sviluppo e il rilascio, in particolare qualsiasi utilizzo di dati di produzione in sistemi non produttivi.

3. Obiettivi

3.1 Prevenire l'introduzione di difetti di sicurezza o vulnerabilità nel software sviluppato su misura o da terze parti.

3.2 Garantire che le pratiche di programmazione sicura e la prevenzione delle vulnerabilità siano integrate in ogni fase del ciclo di vita dello sviluppo dei sistemi.

3.3 Ridurre i rischi associati all'uso di componenti open source o di terze parti imponendo adeguata verifica preliminare e tracciamento.

3.4 Richiedere la revisione formale del codice e i test di sicurezza delle applicazioni prima del rilascio.

3.5 Controllare l'accesso agli ambienti di sviluppo e garantire la separazione dai sistemi di produzione in esercizio.

3.6 Soddisfare i requisiti obbligatori previsti da standard e regolamenti internazionali (ad es. ISO/IEC 27001, GDPR, DORA, NIS2).

4. Ruoli e responsabilità

4.1 Direttore generale

4.1.1 Approva la presente politica e ne è il titolare.

4.1.2 Garantisce che tutte le attività di sviluppo software, interne o esternalizzate, siano conformi alla presente politica.

4.1.3 Riesamina e firma i contratti di sviluppo o di servizio che includono clausole di sviluppo sicuro.

4.1.4 Verifica la conformità dei fornitori tramite controlli periodici o richiedendo evidenze di sicurezza.

4.2 Sviluppatore interno o titolare dell'applicazione

4.2.1 Segue pratiche di programmazione sicura e procedure di rilascio sicure.

4.2.2 Applica la checklist di sviluppo sicuro a ogni progetto.

4.2.3 Convalida la sicurezza di qualsiasi componente open source o di terze parti utilizzato.

4.2.4 Segnala immediatamente al Direttore generale eventuali vulnerabilità individuate.

[... 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 sottoposta a riesame da parte del Direttore generale almeno una volta all'anno per:

9.1.1 verificare il mantenimento della conformità con ISO/IEC 27001, GDPR, NIS2 e DORA

9.1.2 recepire l'evoluzione delle minacce o i cambiamenti nelle migliori pratiche di sviluppo sicuro

9.1.3 garantire la compatibilità con eventuali nuovi strumenti, piattaforme o rapporti con i fornitori

9.2 Riesami intermedi devono essere attivati da:

9.2.1 qualsiasi incidente di sicurezza delle informazioni relativo al software segnalato

9.2.2 introduzione di un nuovo framework di sviluppo o di una nuova piattaforma di hosting

9.2.3 modifica dei partner terzi di sviluppo

9.2.4 aggiornamenti normativi che incidano sugli obblighi relativi al software o alla sicurezza

9.3 Tutte le modifiche alla presente politica devono essere:

9.3.1 documentate con data, sintesi della modifica e approvazione del Direttore generale

9.3.2 comunicate in modo chiaro a tutto il personale di sviluppo interno ed esterno

9.3.3 conservate nell'ambito del controllo delle versioni e della cronologia delle versioni delle politiche dell'organizzazione

9.4 Le versioni aggiornate devono essere rese facilmente accessibili, tramite piattaforme interne, documentazione cartacea o servizi cloud accessibili ai fornitori.

10. Politiche correlate e collegamenti

10.1 La presente politica supporta e dipende dalla corretta applicazione di diverse altre politiche SME:

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: stabilisce la responsabilità per l'assegnazione e la verifica dei controlli di sicurezza dello sviluppo tra progetti e fornitori.

10.1.2 P4S – Politica di controllo degli accessi: fornisce le regole di base per limitare l'accesso agli ambienti di sviluppo e ai repository del codice, inclusa la segregazione dei compiti.

10.1.3 P8S – Politica di consapevolezza e formazione sulla sicurezza delle informazioni: garantisce che gli sviluppatori interni e i collaboratori esterni comprendano le pratiche di sviluppo sicuro e le relative responsabilità di sicurezza.

10.1.4 P17S – Politica di protezione dei dati e privacy: chiarisce come i dati personali devono essere trattati durante i processi di sviluppo, test e registrazione per mantenere la conformità al GDPR.

10.1.5 P30S – Politica di risposta agli incidenti (P30): definisce come gli incidenti di sicurezza connessi allo sviluppo devono essere segnalati, valutati e corretti, incluse le esposizioni relative al codice.

10.2 Tali politiche operano congiuntamente per garantire che lo sviluppo sicuro sia realizzabile e verificabile, anche in un'organizzazione piccola o con limitate competenze tecniche.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede l'attuazione di controlli operativi, incluso lo sviluppo sicuro, allineati agli obiettivi aziendali e al profilo di rischio.

11.2 ISO/IEC 27002

11.2.1 Controllo 8.25 – Raccomanda di integrare la sicurezza nell'intero ciclo di vita del software, incluso il controllo del codice sorgente, il controllo delle versioni e l'accesso degli sviluppatori.

11.2.2 Controllo 8.26 – Specifica i metodi per il test delle applicazioni e la verifica delle funzionalità di sicurezza prima della messa in esercizio in produzione.

11.2.3 Controllo 8.27 – Richiede che gli sviluppatori terzi aderiscano agli stessi standard di sviluppo e che le loro responsabilità di sicurezza siano chiaramente definite.

11.3 NIST SP 800-53 Rev.5

11.3.1 Da SA-3 a SA-15 – Definiscono processi di sviluppo sicuro, incluso il controllo degli accessi degli sviluppatori, i test, la modellazione delle minacce e la documentazione.

11.3.2 SI-10 – Richiede agli sviluppatori di individuare e mitigare le comuni debolezze del software e di utilizzare strumenti automatizzati ove applicabile.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 25 – La “protezione dei dati fin dalla progettazione e per impostazione predefinita” impone l'integrazione di misure di sicurezza e di tutela della privacy durante la progettazione e lo sviluppo del software, in particolare quando vengono trattati dati personali.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(a), (e) e (h) – Richiede politiche di sviluppo sicuro, supervisione sull'uso di componenti open source e documentazione della mitigazione dei rischi connessi alle applicazioni nei soggetti essenziali e importanti.

11.6 DORA UE (2022/2554)

11.6.1 Articoli 6(7), 9(1)(c) e 10(2)(c) – Impongono obblighi di sicurezza del ciclo di vita dello sviluppo per i soggetti del settore finanziario, incluse le PMI, in particolare per i sistemi ICT critici.

11.7 COBIT 2019

11.7.1 BAI03 – “Gestione dell'identificazione e dello sviluppo delle soluzioni” supporta l'applicazione di controlli di sviluppo strutturati che enfatizzano sicurezza, tracciabilità e resilienza, adattati ai vincoli delle PMI.