					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P28					Titolo del documento: **Politica sullo sviluppo esternalizzato**							
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 8.1	N/A
ISO/IEC 27002:2022	Controls 5.19-5.22, 8	N/A
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N/A
GDPR UE	Articoli 28, 32	N/A
NIS2 UE	Articoli 21(2)(a), (h), 23	N/A
DORA UE	Articoli 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Finalità

1.1 La presente politica definisce i controlli obbligatori per l'esternalizzazione dello sviluppo software o di sistemi a fornitori esterni, appaltatori o agenzie, assicurando che pratiche di sicurezza adeguate siano integrate nell'intero ciclo di vita dello sviluppo.

1.2 La politica ha l'obiettivo di prevenire vulnerabilità di sicurezza, perdita di dati, esposizione della proprietà intellettuale (IP) e violazioni di conformità derivanti da incarichi di sviluppo esterno.

1.3 La politica stabilisce requisiti vincolanti in materia di governance dei fornitori, standard di programmazione sicura, gestione degli accessi, obblighi di monitoraggio e dismissione degli accessi alla cessazione del contratto, al fine di preservare riservatezza, integrità e disponibilità (CIA) del software sviluppato.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le unità organizzative che si avvalgono di soggetti esterni per lo sviluppo software o di sistemi, inclusi:

2.1.1 applicazioni web, app mobili, sistemi embedded, API, script, workflow di automazione o moduli di piattaforma

2.1.2 sviluppo personalizzato per piattaforme interne, sistemi rivolti ai clienti o prodotti commerciali

2.1.3 incarichi affidati a sviluppatori terzi, freelance, agenzie o team offshore

2.2 La politica disciplina inoltre qualsiasi soggetto esterno che acceda al codice sorgente, agli ambienti di test o alle pipeline CI/CD durante lo sviluppo.

2.3 I requisiti sono vincolanti indipendentemente dalla tipologia contrattuale, dalla metodologia di sviluppo o dalla localizzazione geografica del fornitore esterno.

3. Obiettivi

3.1 Applicare pratiche di ciclo di vita dello sviluppo sicuro (SDLC) in tutti gli incarichi esternalizzati, dalla pianificazione alla validazione successiva al deployment.

3.2 Assicurare che tutti i contratti con sviluppatori esterni includano clausole obbligatorie relative alla protezione dei dati, alla programmazione sicura e alla titolarità della proprietà intellettuale.

3.3 Definire i requisiti di controllo degli accessi, monitoraggio e audit per gli sviluppatori terzi che interagiscono con i sistemi interni.

3.4 Proteggere l'organizzazione dalle minacce alla supply chain, dalle violazioni normative e dai danni reputazionali connessi al software sviluppato esternamente.

3.5 Mantenere la conformità continua ai quadri di riferimento di sicurezza, inclusi ISO/IEC 27001, NIST, GDPR, NIS2, DORA e COBIT 2019.

4. Ruoli e responsabilità

4.1 Direzione aziendale

4.1.1 Approva i progetti di sviluppo esternalizzato ad alto rischio e convalida le eccezioni alla politica quando giustificate.

4.1.2 Assicura che le decisioni di esternalizzazione siano allineate agli obiettivi strategici e alla propensione al rischio aziendale.

4.2 Responsabile della sicurezza delle informazioni (CISO)

4.2.1 Approva l'onboarding dei fornitori dal punto di vista della sicurezza.

4.2.2 Definisce i requisiti dei controlli di sicurezza per gli incarichi esternalizzati e riesamina le segnalazioni di incidente.

[... 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 almeno una volta all'anno o con maggiore frequenza nelle seguenti circostanze:

9.1.1 introduzione di nuovi modelli di esternalizzazione dello sviluppo, nuovi fornitori o nuove giurisdizioni

9.1.2 aggiornamenti dei quadri normativi quali GDPR, NIS2 o DORA

9.1.3 a seguito di un incidente di sicurezza che coinvolga codice esternalizzato, accessi o deliverable

9.1.4 nell'ambito delle risultanze dell'audit interno o dei miglioramenti del SGSI

9.2 Il Responsabile della sicurezza delle informazioni (CISO) è responsabile dell'avvio e del coordinamento del riesame della politica, in consultazione con:

9.2.1.1 Funzione Legale e Compliance e Funzione Acquisti (per l'allineamento dell'applicazione contrattuale)

9.2.1.2 Responsabili di progetto e di prodotto (per la fattibilità operativa)

9.2.1.3 Funzione Sicurezza delle informazioni (per l'aggiornamento di minacce e controlli)

9.2.1.4 Direzione aziendale (per l'approvazione finale)

9.3 Tutti gli aggiornamenti della politica devono essere:

9.3.1.1 sottoposti a controllo di versione e archiviati in un repository documentale designato

9.3.1.2 comunicati alle parti interessate coinvolte nelle attività di sviluppo esternalizzato

9.3.1.3 collegati a eventuali aggiornamenti delle politiche correlate o della documentazione procedurale

9.4 Un registro delle modifiche deve accompagnare ciascuna versione della politica per garantire la tracciabilità delle modifiche e delle approvazioni.

10. Politiche correlate e collegamenti

10.1 La presente politica supporta ed è supportata dai seguenti documenti correlati:

10.1.1 P1 - Politica per la sicurezza delle informazioni: stabilisce i principi di sicurezza a livello aziendale applicabili ai contesti di sviluppo interni e di terze parti.

10.1.2 P5 - Politica di gestione delle modifiche: assicura che tutte le modifiche connesse al deployment provenienti da codebase esternalizzate siano riesaminate e approvate prima dell'applicazione.

10.1.3 P13 - Politica di classificazione ed etichettatura dei dati: stabilisce come identificare i dati sensibili prima che siano esposti a fornitori di sviluppo o repository.

10.1.4 P18 - Politica sui controlli crittografici: definisce come chiavi, secret e credenziali sensibili devono essere gestiti durante lo sviluppo e la consegna.

10.1.5 P24 - Politica sullo sviluppo sicuro: definisce i requisiti di baseline per le pratiche di sviluppo software interne ed esterne.

10.1.6 P30 - Politica di risposta agli incidenti (P30): disciplina le modalità con cui violazioni o problemi di sicurezza che coinvolgono lo sviluppo esternalizzato devono essere oggetto di escalation, indagine e risoluzione.

10.1.7 P33 - Politica di monitoraggio dell'audit e della conformità: fornisce i requisiti per il riesame delle attività di sviluppo esternalizzato durante gli audit o i riesami di conformità.

11. Standard e quadri di riferimento

11.1 La presente politica è allineata ai quadri di riferimento e alle normative di sicurezza riconosciuti a livello internazionale, al fine di garantire l'esternalizzazione sicura dello sviluppo software e pratiche adeguate di gestione dei fornitori.

11.2 ISO/IEC 27001

11.2.1 Clausola 8.1 - Pianificazione e controllo operativi: impone controlli di processo per lo sviluppo sicuro e l'erogazione da parte di terzi.

11.3 ISO/IEC 27002:2022 - Controlli da 5.19 a 5.21, 8

11.3.1 Allegato A Controllo 5.19 - Sicurezza delle informazioni nei rapporti con i fornitori: richiede accordi formali con clausole di sicurezza e conformità.

11.3.2 Allegato A Controllo 5.20 - Gestione della sicurezza delle informazioni negli accordi con i fornitori: assicura che nei contratti siano integrati controlli specifici per lo sviluppo.

11.3.3 Allegato A Controllo 5.21 - Gestione della sicurezza delle informazioni nella supply chain ICT: prevede il monitoraggio dei deliverable e dei rischi dello sviluppo di terze parti.

11.3.4 Allegato A Controllo 8.27 - Sviluppo esternalizzato: richiede requisiti di sicurezza definiti e controllo degli accessi sul software sviluppato esternamente.

11.3.5 Tali controlli definiscono requisiti strutturati per la selezione, la contrattualizzazione e la supervisione degli sviluppatori esternalizzati, comprese pratiche di sviluppo sicuro, gestione del codice e validazione delle prestazioni.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Processo di acquisizione: richiede che i requisiti di sviluppo sicuro siano definiti al momento dell'acquisizione.

11.4.2 SA-9 - Servizi di sistemi esterni: disciplina il modo in cui gli sviluppatori terzi interagiscono in sicurezza con i servizi interni.

11.4.3 SA-10 - Gestione della configurazione dello sviluppatore: è allineato agli obblighi relativi a controllo di versione, accesso al codice e tracciamento delle modifiche per i team esterni.

11.5 GDPR UE (2016/679)

11.5.1 Articolo 28 - Obblighi del responsabile del trattamento: richiede che i contratti con sviluppatori terzi specifichino requisiti di sicurezza, controllo e audit per il trattamento dei dati personali.

11.5.2 Articolo 32 - Sicurezza del trattamento: impone misure di sicurezza adeguate (ad esempio cifratura, controllo degli accessi) nello sviluppo di sistemi che trattano dati personali.

11.6 Direttiva NIS2 UE (2022/2555)

11.6.1 Articoli 21(2)(a), (h), 23: impongono l'applicazione di pratiche di sviluppo sicuro negli incarichi con terze parti e nelle supply chain digitali, con supervisione e verifica tecnica.

11.7 DORA UE (2022/2554)

11.7.1 Articoli 28(1), (2): richiedono agli enti finanziari di gestire il rischio ICT di terze parti mediante controlli contrattuali e supervisione dello sviluppo sicuro, in particolare per lo sviluppo esternalizzato critico.

11.8 COBIT 2019

11.8.1 APO10 - Gestire i fornitori: stabilisce requisiti strutturati per la valutazione dei fornitori, i contratti e il monitoraggio delle prestazioni.

11.8.2 BAI03 - Gestire lo sviluppo delle soluzioni: corrisponde direttamente ai processi SDLC sicuri, ai riesami del codice e alla validazione dello sviluppo.

11.8.3 DSS05 - DSS05: è allineato al monitoraggio e alla protezione dei sistemi sviluppati esternamente o da terze parti.