| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inserire qui la denominazione dell'entità giuridica registrata | | | | | | | |
| Numero del documento:<br>P28S | | | | | Titolo del documento:<br>**Politica sullo sviluppo esternalizzato** | | | | | | | |
| Versione:<br>1.0 | | Data di entrata in vigore:<br>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 regolamenti

| Standard/Regolamento | Clausola/Articolo | Commento |
|---|---|---|
| ISO/IEC 27001:2022 | Clausole 5.1, 6.1, 8 | Controlli applicabili del SGSI e controlli relativi ai fornitori |
| ISO/IEC 27002:2022 | Controlli 5.19, 5.20, 8.25–8.27 | Controlli sui fornitori e sul ciclo di vita dello sviluppo sicuro |
| NIST SP 800-53 Rev.5 | SA-4, SA-9, SA-11, SA-15, SR-3 | Requisiti relativi ad acquisizione, catena di fornitura, sviluppo sicuro e accordi con i fornitori |
| GDPR UE | Articolo 28 | Requisiti contrattuali e di protezione dei dati per il trattamento effettuato da terze parti |
| NIS2 UE | Articolo 21(2)(a), (h) | Controlli sulla catena di fornitura e sullo sviluppo sicuro delle applicazioni |
| DORA UE | Articolo 10 | Gestione del rischio ICT di terze parti, incluso lo sviluppo esternalizzato |
| COBIT 2019 | BAI03, DSS05 | Requisiti per lo sviluppo esterno e per i fornitori esterni di servizi IT |

**1. Finalità**

1.1 La presente politica garantisce che tutto lo sviluppo software esternalizzato, svolto da freelance, agenzie o fornitori terzi, sia eseguito in modo sicuro, disciplinato contrattualmente e allineato ai requisiti legali, normativi e di audit applicabili.

1.2 La politica tutela l'organizzazione dai rischi connessi a codice non sicuro, titolarità non chiaramente definita, esposizione dei dati e gestione inadeguata dei fornitori, imponendo standard di sviluppo vincolanti e adeguata supervisione sui fornitori, anche in assenza di un dipartimento IT dedicato.

1.3 La presente politica supporta la certificazione ISO/IEC 27001:2022 definendo in modo chiaro le aspettative di sviluppo, le responsabilità e i controlli documentati sulle attività di sviluppo svolte da terze parti.

**2. Ambito di applicazione**

**2.1 La presente politica si applica a:**

2.1.1 Tutti gli sviluppatori esternalizzati, inclusi freelance e agenzie di sviluppo

2.1.2 Qualsiasi attività di sviluppo che coinvolga strumenti interni, siti web esposti pubblicamente, applicazioni software o automazione aziendale

2.1.3 Il personale responsabile della selezione, gestione o supervisione degli sviluppatori esterni

2.1.4 Qualsiasi integrazione con sistemi di terze parti, attività di scripting o sviluppo che interagisca con dati o sistemi aziendali

2.2 Rientrano inoltre nell'ambito di applicazione tutte le parti o piattaforme con accesso a credenziali aziendali, archivi di dati, repository del codice sorgente, ambienti di staging o sistemi di produzione.

**3. Obiettivi**

3.1 Garantire che tutto lo sviluppo esternalizzato rispetti i principi di programmazione sicura e che gli sviluppatori siano vincolati contrattualmente al rispetto di norme documentate e clausole di riservatezza.

3.2 Stabilire la titolarità di tutti i deliverable, compresi codice, asset, credenziali e documentazione, assicurando il pieno trasferimento dei diritti all'azienda e una consegna tracciabile al completamento del progetto.

3.3 Prevenire i rischi di sviluppo più comuni, inclusi il riutilizzo di codice proprietario, gli attacchi alla catena di fornitura tramite librerie, l'uso di framework non supportati e gli accessi amministrativi non verificati.

3.4 Richiedere documentazione preliminare per ogni progetto esternalizzato, inclusi contratto, accordo di riservatezza e requisiti minimi di sicurezza.

3.5 Proteggere i dati dei clienti, i sistemi e i processi interni imponendo adeguata supervisione dello sviluppo, test successivi alla consegna e gestione sicura degli accessi ai sistemi.

## 4. Ruoli e responsabilità

### 4.1 Direttore Generale (GM)

4.1.1 Approva tutti i rapporti con i fornitori e sottoscrive gli accordi di sviluppo.

4.1.2 Garantisce che tutto lo sviluppo esternalizzato sia conforme alla presente politica.

4.1.3 Revoca gli accessi ai sistemi aziendali al completamento del progetto.

4.1.4 Riesamina la documentazione e i risultati successivi alla consegna.

### 4.2 Responsabile di progetto (di norma un dipendente interno o un coordinatore designato)

4.2.1 Gestisce il coordinamento operativo quotidiano con lo sviluppatore esterno.

4.2.2 Verifica che i requisiti funzionali siano soddisfatti e che i deliverable siano testati.

4.2.3 Garantisce la consegna sicura del codice e delle credenziali.

4.2.4 Segnala al GM eventuali problematiche o incidenti connessi allo sviluppo.

[ ... 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 dal Direttore Generale (GM) almeno una volta all'anno. Il riesame garantisce che continui a soddisfare:**

9.1.1.1 I requisiti di certificazione ISO/IEC 27001

9.1.1.2 Le modifiche degli obblighi di conformità (ad es. articolo 28 del GDPR, articolo 10 del DORA)

9.1.1.3 Le attuali pratiche di sviluppo nelle PMI e i rischi di terze parti

### 9.2 Riesami intermedi

**9.2.1 I riesami della politica devono inoltre essere effettuati quando:**

9.2.1.1 Viene avviato l'onboarding di un nuovo fornitore o di una nuova piattaforma per lo sviluppo esternalizzato

9.2.1.2 Si verifica un incidente significativo connesso allo sviluppo esternalizzato

9.2.1.3 Si verificano modifiche significative agli strumenti, alle piattaforme o agli ambienti utilizzati

### 9.3 Processo di riesame

**9.3.1 Il GM è responsabile di:**

9.3.1.1 Verificare che contratti, accordi di riservatezza e processi di controllo degli accessi rimangano efficaci

9.3.1.2 Confermare che i fornitori attuali e i freelance siano allineati alla politica

9.3.1.3 Riesaminare i termini sulla base del feedback derivante da progetti o incidenti precedenti

**9.4 Controllo delle versioni e comunicazione**

**9.4.1 Tutte le modifiche devono essere:**

9.4.1.1 Registrate con data, motivo e descrizione della modifica

9.4.1.2 Approvate dal GM e aggiunte alla cronologia delle versioni

9.4.1.3 Comunicate a tutto il personale o ai Responsabili di progetto che lavorano con sviluppatori esterni

9.4.1.4 Ridistribuite a tutti i fornitori e alle terze parti interessate, ove necessario

## 10. Politiche correlate e collegamenti

**10.1 La presente politica supporta direttamente e dipende dall'applicazione delle seguenti politiche allineate alle esigenze delle PMI:**

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: chiarisce chi è responsabile dell'approvazione dei fornitori, del controllo degli accessi e dell'accettazione del rischio nell'uso di sviluppatori esternalizzati.

10.1.2 P4S – Politica sul controllo degli accessi: definisce la corretta creazione, restrizione e cessazione degli account utente e degli accessi amministrativi utilizzati durante lo sviluppo esternalizzato.

10.1.3 P8S – Politica sulla consapevolezza e formazione in materia di sicurezza delle informazioni: garantisce che il personale interno comprenda come coordinarsi in modo sicuro con gli sviluppatori esterni, inclusa la gestione delle credenziali e dei file di progetto.

10.1.4 P17S – Politica di protezione dei dati e privacy: stabilisce i requisiti di sicurezza e legali per il trattamento dei dati personali che possono essere trattati dagli sviluppatori esternalizzati ai sensi del GDPR.

10.1.5 P24S – Politica sullo sviluppo sicuro: specifica come lo sviluppo interno ed esterno debba seguire pratiche di programmazione sicura e la verifica di librerie e framework.

10.1.6 P30S – Politica di risposta agli incidenti: si applica quando lo sviluppo esternalizzato provoca incidenti di sicurezza delle informazioni o vulnerabilità, guidando indagini e azioni di rimedio coordinate.

10.2 Tali politiche devono essere applicate congiuntamente per garantire che lo sviluppo esternalizzato non generi rischi non gestiti né comporti violazioni degli obblighi di conformità delle PMI.

## 11. Standard e quadri di riferimento

**11.1 ISO/IEC 27001**

11.1.1 Clausola 6.1 – Le organizzazioni devono valutare e trattare i rischi per la sicurezza delle informazioni associati ai fornitori.

11.1.2 Clausola 8.1 – Richiede pianificazione e controllo operativi, inclusi i servizi di terze parti come lo sviluppo esternalizzato.

**11.2 ISO/IEC 27002**

11.2.1 Controllo 5.19 – Raccomanda di valutare la capacità dei fornitori di soddisfare i requisiti di sicurezza delle informazioni.

11.2.2 Controllo 5.20 – Incoraggia il monitoraggio regolare e il riesame periodico dei servizi di terze parti.

11.2.3 Controlli 8.25–8.27 – Definiscono pratiche del ciclo di vita dello sviluppo sicuro applicabili allo sviluppo esternalizzato.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 SA-4 – Richiede che le strategie di acquisizione includano misure di sicurezza delle informazioni.

11.3.2 SA-9 – Riguarda lo sviluppo di sistemi esterni e i rischi della catena di fornitura.

11.3.3 SA-11 – Definisce pratiche di sviluppo sicuro, incluse la revisione del codice e la correzione dei difetti.

11.3.4 SA-15 – Promuove l'uso di strumenti automatizzati per il rilevamento dei difetti e l'assurance del software.

11.3.5 SR-3 – Richiede che gli accordi con i fornitori includano requisiti di cybersicurezza.

**11.4 Regolamento generale sulla protezione dei dati (GDPR)**

11.4.1 Articolo 28 – Richiede contratti con i responsabili del trattamento terzi per garantire adeguate misure di protezione dei dati, direttamente applicabili agli sviluppatori che trattano o accedono a dati personali.

**11.5 Direttiva UE NIS2 (2022/2555)**

11.5.1 Articolo 21(2)(a), (h) – Richiede controlli di sicurezza della catena di fornitura e pratiche di sviluppo software sicuro per i fornitori di servizi digitali rientranti nell'ambito di applicazione, incluse le PMI quando applicabile.

**11.6 Regolamento UE Digital Operational Resilience Act (DORA)**

11.6.1 Articolo 10 – Richiede la gestione del rischio ICT di terze parti, inclusi accordi di sviluppo, obblighi di sicurezza e controlli del rischio relativi ai fornitori terzi.

**11.7 COBIT 2019**

11.7.1 BAI03 – Gestione dell'identificazione e dello sviluppo delle soluzioni – Garantisce che lo sviluppo esterno soddisfi i requisiti aziendali e le aspettative di sicurezza.

11.7.2 DSS05 – Gestire i servizi di sicurezza – Richiede che i fornitori esterni di servizi di sicurezza e di sviluppo operino nel rispetto delle regole di sicurezza applicabili e sotto adeguata supervisione.