					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P26S					Titolo del documento: **Politica di sicurezza per terze parti e fornitori P26S**							
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

Standard/Normativa	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Controlli operativi per i rapporti con terze parti e fornitori
ISO/IEC 27002:2022	Controlli 5.19–5.22	Controlli di sicurezza dei fornitori, clausole contrattuali di sicurezza, gestione delle modifiche, monitoraggio e riesame
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Acquisizione, configurazione, accordi di interconnessione e controlli sul personale esterno
GDPR UE	Articoli 28, 32	Accordi sul trattamento dei dati, requisiti di sicurezza per i responsabili del trattamento
NIS2 UE	Articoli 21(2)(a)(b)(i), 23(1)	Gestione del rischio della catena di fornitura, supervisione dei servizi di terze parti
DORA UE	Articoli 5(1)(2), 28(1)(2)	Gestione del rischio ICT per i fornitori terzi di servizi
COBIT 2019	APO10, APO12, DSS05	Gestione dei fornitori e integrazione del rischio

1. Finalità

1.1 La presente politica stabilisce i requisiti di sicurezza obbligatori per l'avvio, la gestione e la cessazione dei rapporti con terze parti e fornitori che accedono ai dati, ai sistemi o ai servizi dell'organizzazione o che possono influire su di essi.

1.2 Essa garantisce che i fornitori esterni, inclusi i fornitori di supporto IT, i fornitori di servizi cloud, gli sviluppatori software e gli appaltatori di processi aziendali, trattino gli asset aziendali in modo sicuro e in conformità alle leggi e agli standard applicabili.

1.3 La presente politica riduce rischi quali perdita di dati, modifiche non autorizzate ai sistemi, sanzioni normative o interruzioni operative causate da accordi con terze parti non sicuri o non adeguatamente governati.

2. Ambito di applicazione

2.1 La presente politica si applica a tutte le terze parti che:

2.1.1 Forniscono software, infrastrutture, servizi di hosting o servizi cloud

2.1.2 Accedono a sistemi, dispositivi o applicazioni interni, oppure li gestiscono

2.1.3 Trattano dati, documenti o backup aziendali

2.1.4 Supportano le operazioni aziendali, le risorse umane, la finanza o i servizi ai clienti

2.2 Si applica inoltre a:

2.2.1 Il personale interno coinvolto nella selezione, nell'ingaggio o nella supervisione dei fornitori

2.2.2 Chiunque gestisca l'onboarding dei fornitori, i contratti, gli accessi o i riesami

2.2.3 Qualsiasi sistema o processo che dipenda da componenti o servizi di terze parti

3. Obiettivi

3.1 Garantire che tutti i fornitori soddisfino requisiti di sicurezza chiaramente definiti.

3.2 Richiedere che i contratti con i fornitori includano obblighi vincolanti in materia di sicurezza, protezione dei dati personali e risposta agli incidenti.

3.3 Valutare e documentare i rischi dei fornitori prima della sottoscrizione degli accordi o della concessione degli accessi.

3.4 Sottoporre a riesame periodico i fornitori critici o ad alto rischio per confermarne la conformità.

3.5 Stabilire un processo formale per la gestione delle eccezioni, degli incidenti e degli aggiornamenti contrattuali.

3.6 Supportare la conformità agli obblighi di ISO/IEC 27001:2022, GDPR, NIS2 e DORA relativi alla governance dei fornitori.

4. Ruoli e responsabilità

4.1 Direttore Generale (GM)

4.1.1 Ha la responsabilità finale della selezione dei fornitori e della conformità ai requisiti di sicurezza

4.1.2 Approva i contratti, le eccezioni e le escalation che coinvolgono i fornitori

4.1.3 Sovraintende alla risposta agli incidenti e al processo decisionale nei casi in cui i fornitori non rispettino i propri obblighi

4.2 Fornitore IT o referente interno per la sicurezza

4.2.1 Valuta gli accessi tecnici richiesti dai fornitori

4.2.2 Applica le regole di controllo degli accessi, riesamina i log e verifica la gestione sicura dei dati

4.2.3 Riesamina, ove applicabile, le evidenze dei controlli di sicurezza, le certificazioni o i risultati di audit

[... 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 annualmente dal Direttore Generale, con il coinvolgimento del fornitore IT o del responsabile dei fornitori.

9.2 La politica deve inoltre essere riesaminata:

9.2.1 A seguito di qualsiasi modifica significativa degli obblighi legali, normativi o contrattuali

9.2.2 A seguito di un incidente di sicurezza relativo a un fornitore o di un rilievo di audit

9.2.3 In occasione dell'introduzione di nuove categorie di fornitori, ad esempio piattaforme SaaS critiche

9.3 Tutti gli aggiornamenti devono essere:

9.3.1 Documentati con storico delle versioni e relativa motivazione

9.3.2 Approvati dal Direttore Generale

9.3.3 Comunicati al personale interno pertinente e ai responsabili dei fornitori

9.3.4 Conservati insieme alle versioni precedenti in conformità alla P14S – Politica di conservazione e smaltimento dei dati

10. Politiche correlate e collegamenti

10.1 L'efficacia della presente politica dipende dal coordinamento con le seguenti politiche SME sulla sicurezza delle informazioni:

10.1.1 P2S – Politica sui ruoli e sulle responsabilità di governance: assegna la responsabilità della supervisione dei fornitori e dell'applicazione dei contratti.

10.1.2 P4S – Politica di controllo degli accessi: definisce le regole di limitazione degli accessi da applicare quando ai fornitori viene concesso accesso ai sistemi.

10.1.3 P17S – Politica di protezione dei dati e tutela della privacy: garantisce che i fornitori che trattano dati personali rispettino i principi di protezione dei dati e i requisiti di legge.

10.1.4 P14S – Politica di conservazione e smaltimento dei dati: si applica a qualsiasi dato o registrazione condiviso con i fornitori o da essi conservato e disciplina lo smaltimento sicuro dopo la cessazione del contratto.

10.1.5 P30S – Politica di risposta agli incidenti: definisce le modalità di risposta quando un fornitore causa o è coinvolto in un incidente di sicurezza, incluse le procedure di escalation e di gestione delle evidenze.

10.2 Tali politiche operano congiuntamente per garantire il controllo del rischio dei fornitori lungo l'intero ciclo di vita contrattuale.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede l'attuazione di controlli operativi, inclusi quelli applicati ai rapporti con terze parti e fornitori.

11.2 ISO/IEC 27002

11.2.1 Controllo 5.19 – Garantisce che le misure di sicurezza dei fornitori siano allineate ai requisiti dell'organizzazione.

11.2.2 Controllo 5.20 – Richiede accordi formali che coprano termini di sicurezza, responsabilità e obblighi in caso di violazione.

11.2.3 Controllo 5.21 – Disciplina le modifiche ai servizi dei fornitori che possono influire sul livello di sicurezza.

11.2.4 Controllo 5.22 – Richiede il monitoraggio e il riesame dei servizi dei fornitori e della relativa conformità.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Disciplina l'acquisizione di sistemi e servizi esterni, richiedendo valutazioni del rischio e aspettative definite.

11.3.2 SA-10 – Disciplina le procedure di configurazione e gestione delle modifiche che coinvolgono sistemi gestiti da terze parti.

11.3.3 CA-3 – Richiede accordi di interconnessione per sistemi che coinvolgono soggetti esterni.

11.3.4 PS-7 – Definisce requisiti di verifica e responsabilizzazione del personale esterno.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 28 – Richiede accordi sul trattamento dei dati con i fornitori che agiscono come responsabili del trattamento.

11.4.2 Articolo 32 – Impone misure tecniche e organizzative di sicurezza adeguate per tutti i responsabili del trattamento.

11.5 Direttiva NIS2 UE (2022/2555)

11.5.1 Articolo 21(2)(a), (b), (i) – Impone la gestione del rischio della catena di fornitura ICT e controlli sulle terze parti.

11.5.2 Articolo 23(1) – Richiede una supervisione documentata dei servizi di terze parti per i soggetti essenziali e importanti.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 5(1) – Richiede un quadro di riferimento per la gestione del rischio ICT che copra tutti i fornitori terzi critici.

11.6.2 Articolo 5(2) – Stabilisce controlli contrattuali e operativi per le dipendenze dai servizi ICT.

11.6.3 Articolo 28(1), (2) – Definisce regole di supervisione per il rischio ICT derivante da terze parti nel settore finanziario.

11.7 COBIT 2019

11.7.1 APO10 – “Gestire i fornitori” definisce i controlli di approvvigionamento e le aspettative per la gestione dei rapporti.

11.7.2 APO12 – “Gestire il rischio” integra il rischio dei fornitori nella governance del rischio organizzativo.

11.7.3 DSS05 – “Gestire i servizi di sicurezza” si applica ai fornitori terzi gestiti e ai prestatori di servizi in outsourcing.