					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P26					Titolo del documento: **Politica di sicurezza delle terze parti e dei fornitori**							
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 standard e normative

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Pianificazione e controllo operativi: richiede controlli formali sui servizi di terze parti che hanno impatto sul SGSI
ISO/IEC 27002:2022	Controlli 5.19–5.22	Politiche e procedure per i rapporti con i fornitori; Gestione del rischio dei fornitori; Gestione dell'erogazione dei servizi dei fornitori; Monitoraggio e riesame dei fornitori
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Servizi di sistemi esterni; Gestione della configurazione degli sviluppatori; Interconnessioni dei sistemi; Sicurezza del personale di terze parti
GDPR UE	Articoli 28, 32, 33	Obblighi dei responsabili del trattamento, Sicurezza del trattamento, Notifica di una violazione dei dati personali
NIS2 UE	Articolo 21(2)(e–f)	Gestione dei fornitori basata sul rischio e vigilanza sulla sicurezza
DORA UE	Articoli 28, 30	Rischio ICT di terze parti, Vigilanza sui fornitori terzi critici di servizi ICT
COBIT 2019	BAI05, DSS02, MEA03	Gestire l'abilitazione al cambiamento organizzativo; Gestire le richieste di servizio e gli incidenti; Monitorare, valutare e verificare la conformità

1. Finalità

1.1 La presente politica definisce i requisiti di sicurezza delle informazioni per l'instaurazione, la gestione e il mantenimento di rapporti sicuri con fornitori e prestatori di servizi terzi.

1.2 Essa garantisce che tutti i fornitori con accesso ai dati, ai sistemi o all'infrastruttura dell'organizzazione siano soggetti a rigorosi controlli di sicurezza, misure di tutela contrattuale e vigilanza continua lungo l'intero ciclo di vita del servizio.

1.3 La politica supporta i controlli dell'Allegato A della ISO/IEC 27001 dal 5.19 al 5.22, integrando i requisiti di sicurezza nei processi di approvvigionamento e due diligence dei fornitori, onboarding dei fornitori, gestione dei contratti, monitoraggio dei servizi e cessazione del contratto.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti i fornitori terzi, gli appaltatori, i fornitori di servizi cloud e le organizzazioni di servizi che trattano o accedono agli asset informativi dell'organizzazione

2.1.2 tutti i ruoli interni coinvolti nella valutazione dei fornitori, nell'onboarding dei fornitori, nella contrattualizzazione, nella gestione del rischio, nel monitoraggio o nella cessazione del contratto

2.1.3 tutti i rapporti con i fornitori che comprendono accesso a dati sensibili, integrazione con servizi di produzione o supporto a funzioni aziendali critiche

2.2 Sono inclusi sia i fornitori diretti sia, ove applicabile, i relativi subfornitori, nonché software di terze parti, infrastrutture, supporto e servizi gestiti.

3. Obiettivi

3.1 Garantire che i rischi di sicurezza dei fornitori siano identificati, valutati e mitigati in modo coerente lungo l'intero ciclo di vita del rapporto.

3.2 Integrare requisiti di sicurezza standardizzati in tutti i contratti con i fornitori, inclusi gli obblighi di notifica delle violazioni, le clausole di diritto di audit e le responsabilità in materia di protezione dei dati.

3.3 Richiedere una due diligence formale e valutazioni del rischio documentate prima dell'ingaggio di nuovi fornitori o del rinnovo di accordi di servizio ad alto rischio.

3.4 Stabilire meccanismi per il monitoraggio continuo della conformità dei fornitori, inclusi riesami delle prestazioni, audit ed escalation degli incidenti.

3.5 Gestire le modifiche ai servizi dei fornitori e applicare un offboarding sicuro, nonché la restituzione o distruzione dei dati in fase di cessazione.

3.6 Allineare i controlli di sicurezza delle terze parti agli obblighi normativi e contrattuali applicabili, inclusi GDPR, NIS2, DORA e gli standard ISO/IEC 27001.

4. Ruoli e responsabilità

4.1 Responsabile della sicurezza delle informazioni (CISO)

4.1.1 È il titolare della politica e ne garantisce l'allineamento con il SGSI complessivo, la gestione del rischio e la strategia di conformità.

4.1.2 Approva i livelli di classificazione dei fornitori, gli esiti dei riesami di sicurezza e le eccezioni ad alto rischio.

4.1.3 Partecipa all'escalation dei gravi incidenti che coinvolgono i fornitori e alle negoziazioni contrattuali per i servizi critici.

4.2 Approvvigionamento e gestione dei fornitori

4.2.1 Garantisce che tutti i nuovi contratti con i fornitori e i contratti rinnovati includano clausole approvate in materia di sicurezza e protezione dei dati.

4.2.2 Mantiene il registro centralizzato dei fornitori e si coordina con la Funzione legale e compliance per la documentazione relativa al rischio di terze parti.

4.2.3 Avvia i processi di onboarding dei fornitori e ne garantisce l'allineamento con le valutazioni di sicurezza precontrattuali.

[... 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, o prima in caso di:

9.1.1 modifiche sostanziali alla strategia di approvvigionamento o all'ecosistema dei fornitori

9.1.2 aggiornamenti dei quadri normativi o regolamentari (ad esempio DORA, GDPR)

9.1.3 incidenti rilevanti di terze parti, violazioni dei dati o esiti negativi di audit

9.1.4 risultanze di valutazioni del rischio o di organismi esterni di certificazione

9.2 Il processo di riesame è di responsabilità congiunta del CISO, dell'Approvvigionamento, della Funzione legale e delle funzioni di gestione del rischio.

9.3 Tutte le revisioni della politica devono essere documentate nel Registro di controllo documentale del SGSI, sottoposte a controllo di versione e comunicate alle parti interessate pertinenti tramite i canali di governance dei fornitori e i programmi di sensibilizzazione del personale.

9.4 Le versioni superate devono essere archiviate per un periodo minimo di tre anni ai fini della tracciabilità e della conformità legale.

10. Politiche correlate e collegamenti

10.1 P1 – Politica per la sicurezza delle informazioni. Definisce l'impegno generale a proteggere tutte le operazioni dell'organizzazione, inclusa la dipendenza da fornitori terzi e fornitori esterni di servizi IT.

10.2 P6 – Politica di gestione del rischio. Guida l'identificazione, la valutazione e la mitigazione dei rischi associati ai rapporti con terze parti, inclusi i rischi ereditati o sistemici derivanti dagli ecosistemi dei fornitori.

10.3 P17 – Politica di protezione dei dati e privacy. Si applica a tutti i fornitori che trattano dati personali e richiede adeguati termini contrattuali, misure di tutela per i trasferimenti e principi di privacy by design.

10.4 P4 – Politica di controllo degli accessi. Disciplina le modalità con cui il personale di terze parti ottiene accesso ai sistemi dell'organizzazione, applicando autorizzazioni basate sui ruoli, controlli di sessione e procedure di revoca.

10.5 P22 – Politica di registrazione e monitoraggio. Richiede che l'accesso dei fornitori ai sistemi sia monitorato, registrato e riesaminato, in particolare negli ambienti in cui si svolgono attività privilegiate o incentrate sui dati.

10.6 P30 – Politica di risposta agli incidenti (P30). Definisce le procedure di escalation e i requisiti di segnalazione delle violazioni per eventi di sicurezza originati dai fornitori o per indagini congiunte che coinvolgono sistemi di terze parti.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001: Clausola 8.1 – Pianificazione e controllo operativi: richiede controlli formali sui servizi di terze parti che hanno impatto sul SGSI.

11.2 ISO/IEC 27002:2022 – Controlli da 5.19 a 5.22:

11.2.1 Allegato A, Controllo 5.19 – Politiche e procedure per i rapporti con i fornitori: richiede controlli per la gestione delle interazioni con i fornitori.

11.2.2 Allegato A, Controllo 5.20 – Gestione del rischio dei fornitori: si concentra su identificazione, valutazione e vigilanza continua sul livello di sicurezza dei fornitori.

11.2.3 Allegato A, Controllo 5.21 – Gestione dell'erogazione dei servizi dei fornitori: richiede l'allineamento di prestazioni e sicurezza alle aspettative contrattuali.

11.2.4 Allegato A, Controllo 5.22 – Monitoraggio e riesame dei fornitori: rafforza la necessità di validazione continua e rivalutazione della conformità delle terze parti.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Servizi di sistemi esterni: definisce requisiti di sicurezza e di rischio per i sistemi gestiti da soggetti esterni.

11.3.2 SA-10 – Gestione della configurazione degli sviluppatori: si applica quando terze parti forniscono software o ambienti.

11.3.3 CA-3 – Interconnessioni dei sistemi: richiede vigilanza e accordi sui flussi di dati tra sistemi di entità diverse.

11.3.4 PS-7 – Sicurezza del personale di terze parti: garantisce che appaltatori e personale dei fornitori siano sottoposti ad adeguate verifiche e monitoraggio.

11.4 GDPR UE (2016/679):

11.4.1 Articolo 28 – Obblighi dei responsabili del trattamento: richiede accordi scritti con i responsabili del trattamento, incluse misure tecniche e organizzative (TOM).

11.4.2 Articolo 32 – Sicurezza del trattamento: impone adeguate misure di sicurezza sia ai titolari sia ai responsabili del trattamento.

11.4.3 Articolo 33 – Notifica di una violazione dei dati personali: richiede una notifica tempestiva da parte dei fornitori in caso di violazione.

11.5 Direttiva UE NIS2 (2022/2555):

11.5.1 Articolo 21(2)(e–f): richiede la gestione dei fornitori basata sul rischio e la vigilanza sulla sicurezza, in particolare nelle catene di fornitura digitali dei soggetti essenziali e importanti.

11.6 DORA UE (2022/2554):

11.6.1 Articolo 28 – Rischio ICT di terze parti: impone obblighi di valutazione del rischio, termini contrattuali di sicurezza e strategie di uscita per i fornitori di servizi finanziari.

11.6.2 Articolo 30 – Vigilanza sui fornitori terzi critici di servizi ICT: stabilisce aspettative rafforzate di monitoraggio e supervisione per i fornitori chiave.

11.7 COBIT 2019:

11.7.1 BAI05 – Gestire l'abilitazione al cambiamento organizzativo: garantisce che le transizioni dei fornitori siano governate in modo sicuro.

11.7.2 DSS02 – Gestire le richieste di servizio e gli incidenti: si applica alle problematiche segnalate dai fornitori e all'integrazione della gestione degli incidenti.

11.7.3 MEA03 – Monitorare, valutare e verificare la conformità: rafforza la misurazione delle prestazioni dei fornitori e il monitoraggio della conformità.