					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P19S					Titolo del documento: **Politica di gestione delle vulnerabilità e delle patch**							
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 norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	
ISO/IEC 27002:2022	Controlli 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Direttiva UE NIS2	Articoli 21(2)(d), 21(2)(e)	
Regolamento UE DORA	Articoli 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
GDPR UE	Articolo 32(1)(b)	

1. Finalità

1.1 La presente politica definisce le modalità con cui l'organizzazione identifica, valuta e mitiga le vulnerabilità nei sistemi, nelle applicazioni e nell'infrastruttura.

1.2 La finalità è ridurre il rischio di cibersicurezza imponendo l'applicazione tempestiva delle patch e misure di rimedio basate sul rischio, adeguate alle piccole e medie imprese (PMI).

1.3 La presente politica supporta la conformità ai fini della certificazione ISO/IEC 27001:2022 e contribuisce al rispetto degli obblighi normativi previsti dal GDPR, dalla NIS2 e dal DORA, richiedendo la gestione proattiva delle vulnerabilità tecniche.

1.4 L'organizzazione riconosce che i sistemi non aggiornati costituiscono una minaccia significativa per la sicurezza delle informazioni e devono essere gestiti in modo sistematico e tempestivo.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti i server, desktop, laptop, dispositivi mobili, apparati di rete e piattaforme ospitate nel cloud utilizzati dall'organizzazione

2.1.2 Tutti i sistemi operativi, i software di terze parti, i plug-in e le applicazioni utilizzati nelle attività aziendali

2.1.3 Il personale IT interno o i fornitori esterni di servizi IT responsabili della manutenzione, dell'aggiornamento o del monitoraggio dei sistemi

2.1.4 Qualsiasi codice sviluppato su misura o software embedded mantenuto dall'organizzazione o per suo conto

2.2 La politica si applica sia all'infrastruttura gestita direttamente dall'organizzazione sia ai sistemi amministrati da fornitori contrattualizzati o da provider di hosting.

3. Obiettivi

3.1 Identificare e valutare tempestivamente e in modo coerente le vulnerabilità note in tutti gli asset IT aziendali

3.2 Applicare patch e aggiornamenti software in base alla gravità e al rischio per le operazioni dell'organizzazione o per i dati personali

3.3 Prevenire lo sfruttamento di debolezze tecniche che potrebbero causare interruzioni del servizio, violazioni dei dati o mancata conformità normativa

3.4 Mantenere registrazioni accurate delle patch applicate, delle problematiche aperte e delle eccezioni, al fine di garantire la capacità di dimostrare la conformità

3.5 Utilizzare strumenti e processi adeguati alle dimensioni dell'organizzazione e alla sua complessità operativa, senza comprometterne l'efficacia

3.6 Supportare la conformità legale e normativa, incluso l'articolo 32 del GDPR e l'Allegato A, controllo 8, della ISO

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 Ha la responsabilità complessiva di garantire l'attuazione delle attività di applicazione delle patch e di gestione delle vulnerabilità

4.1.2 Approva le eccezioni al rischio nei casi in cui le patch non possano essere applicate e riesamina le relative misure di mitigazione

4.1.3 Riesamina i report sullo stato di applicazione delle patch e garantisce la disponibilità delle risorse necessarie per rispettare gli obblighi in materia

4.2 Fornitore di supporto IT / amministratore IT interno

4.2.1 Monitora i sistemi per individuare vulnerabilità e patch disponibili mediante avvisi dei fornitori, bollettini sulle minacce e notifiche a livello di sistema operativo

4.2.2 Applica gli aggiornamenti del sistema operativo, del firmware e delle applicazioni entro le tempistiche definite

4.2.3 Mantiene un registro formale delle patch e documenta gli aggiornamenti non risolti o rinviati

4.2.4 Esegue test e pianifica gli aggiornamenti critici per ridurre al minimo l'interruzione operativa

[... 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 almeno una volta all'anno dal Direttore generale, con il contributo del fornitore di supporto IT e del Coordinatore privacy

9.2 Trigger di riesame

9.2.1 Devono essere effettuati riesami intermedi se:

9.2.1.1 Una vulnerabilità rilevante o un exploit interessa i sistemi inclusi nell'ambito di applicazione

9.2.1.2 Si verificano modifiche significative ai sistemi o al software

9.2.1.3 Un audit identifica carenze nei processi di applicazione delle patch

9.2.1.4 Viene registrato un incidente o una violazione correlati all'applicazione delle patch

9.3 Controllo delle versioni della politica

9.3.1 Tutti gli aggiornamenti devono essere registrati in un registro delle modifiche con il relativo riepilogo

9.3.2 Le modifiche devono essere comunicate al personale interessato

9.3.3 Le versioni obsolete devono essere archiviate con accesso ristretto

10. Politiche correlate e collegamenti

10.1 La presente politica supporta ed è collegata a diverse altre politiche SME:

10.1.1 P12S – Politica di gestione degli asset: identifica la titolarità e la classificazione dei sistemi, garantendo che tutti gli asset che richiedono patch siano censiti e inclusi nell'inventario

10.1.2 P14S – Politica di conservazione e smaltimento dei dati: garantisce che i sistemi pianificati per la dismissione siano aggiornati in sicurezza o sottoposti a cancellazione sicura, riducendo l'esposizione alle vulnerabilità

10.1.3 P17S – Politica di protezione dei dati e privacy: assegna priorità al rimedio delle vulnerabilità per i sistemi che trattano dati personali al fine di rispettare la normativa sulla privacy

10.1.4 P22S – Politica di registrazione e monitoraggio: supporta il rilevamento di sistemi non aggiornati o di comportamenti sospetti che possano indicare lo sfruttamento di una vulnerabilità

10.1.5 P30S – Politica di risposta agli incidenti: definisce le procedure per rispondere alle vulnerabilità che si traducono in incidenti di sicurezza, incluse le fasi di escalation e segnalazione

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede l'implementazione di controlli per affrontare il rischio operativo, inclusa la gestione delle vulnerabilità

11.2 ISO/IEC 27002

11.2.1 Controllo 8.8 – Specifica processi per l'esecuzione di scansioni e la correzione di debolezze note nei sistemi

11.2.2 Controllo 8.9 – Sottolinea l'importanza della configurazione sicura, della convalida delle patch e del controllo delle modifiche per evitare nuove esposizioni durante gli aggiornamenti

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Richiede l'identificazione delle vulnerabilità e il relativo rimedio entro tempistiche definite

11.3.2 SI-2 – Richiede l'applicazione tempestiva delle patch e degli aggiornamenti in base alla gravità

11.3.3 CM-2 – Disciplina le configurazioni baseline dei sistemi e la documentazione degli aggiornamenti per garantire misure di protezione coerenti

11.4 GDPR UE

11.4.1 Articolo 32(1)(b) – Richiede alle organizzazioni di implementare misure tecniche adeguate, inclusa l'applicazione delle patch, per mantenere la sicurezza del trattamento

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(d) – Richiede il trattamento delle vulnerabilità mediante scansioni sistematiche e attività di rimedio

11.5.2 Articolo 21(2)(e) – Impone la configurazione sicura e la gestione delle patch per garantire la resilienza ICT

11.6 Regolamento UE DORA

11.6.1 Articolo 8(1) – Richiede il rilevamento e la mitigazione dei rischi ICT, incluse le vulnerabilità tecniche

11.6.2 Articolo 10(2) – Impone ai soggetti finanziari di correggere le debolezze che incidono sui sistemi ICT e sulle operazioni

11.7 COBIT 2019

11.7.1 DSS05.02 – Richiede il trattamento delle vulnerabilità tecniche note per mantenere operazioni sicure

11.7.2 APO12.01 – Allinea la gestione del rischio con il monitoraggio proattivo e la correzione delle debolezze dei sistemi