					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P20S					Titolo del documento: **Protezione degli endpoint - Politica sul malware**							
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/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 8	Controlli operativi per la protezione dal malware
ISO/IEC 27002:2022	Controllo 8	Misure di controllo per la protezione degli endpoint
NIST SP 800-53 Rev.5	SI-3, SI-4	Protezione dal codice malevolo e risposta agli incidenti
Direttiva UE NIS2	Articoli 21(2)(d), (e)	Malware e gestione del rischio per soggetti essenziali e importanti
Regolamento UE DORA	Articoli 10(1), 15	Resilienza operativa e verifica delle terze parti
COBIT 2019	DSS05.02, DSS05.04	Protezione e monitoraggio di endpoint e rete
Regolamento UE GDPR	Articoli 32(1)(b), 33	Misure tecniche e organizzative e notifica delle violazioni

1. Finalità

1.1 La presente politica definisce i requisiti minimi tecnici, procedurali e comportamentali per la protezione di tutti i dispositivi endpoint, quali laptop, desktop, dispositivi mobili e supporti rimovibili, dal codice malevolo, inclusi virus, ransomware, spyware, rootkit e altre minacce malware.

1.2 La finalità è garantire che gli endpoint siano dotati delle necessarie misure di protezione, mantenuti e utilizzati in modo da ridurre il rischio di infezione da malware, di propagazione e di compromissione dei sistemi.

1.3 L'organizzazione riconosce che gli endpoint costituiscono comuni punti di ingresso del malware e devono pertanto essere sottoposti ad hardening, monitorati e protetti mediante un approccio di difesa in profondità.

1.4 La politica supporta gli obiettivi di certificazione ISO/IEC 27001:2022 dell'organizzazione ed è allineata al Regolamento generale sulla protezione dei dati (GDPR), alla Direttiva NIS2, al Digital Operational Resilience Act (DORA) e ad altri quadri di riferimento pertinenti.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 Tutti gli endpoint dell'organizzazione, inclusi desktop, laptop, tablet, telefoni mobili e terminali punto vendita

2.1.2 Dispositivi personali (Bring Your Own Device - BYOD) utilizzati per accedere ad applicazioni aziendali o dati

2.1.3 Dispositivi di archiviazione rimovibili quali unità USB e dischi rigidi esterni

2.1.4 Qualsiasi sistema operativo, software endpoint o strumento di comunicazione in esecuzione su tali piattaforme

2.2 Si applica inoltre a:

2.2.1 Personale interno, collaboratori esterni, tirocinanti e fornitori di servizi gestiti

2.2.2 Dispositivi utilizzati in sede, da remoto o nell'ambito di modalità di lavoro ibrido

2.2.3 Endpoint connessi al cloud o offline che archiviano dati aziendali o dati personali

3. Obiettivi

3.1 Prevenire l'infezione da malware e la sua propagazione nei sistemi interni, nei dispositivi degli utenti e nelle connessioni esterne

3.2 Rilevare e contenere rapidamente le minacce connesse al malware mediante tecnologie automatizzate di sicurezza degli endpoint e processi di escalation definiti

3.3 Garantire che solo dispositivi autorizzati, protetti e monitorati siano utilizzati per accedere alle informazioni aziendali

3.4 Stabilire responsabilità chiare del personale e regole di comportamento degli utenti per ridurre il rischio di incidenti correlati al malware

3.5 Mantenere registrazioni tracciabili e verificabili dei rilevamenti di malware, delle risposte adottate e della conformità alla politica

3.6 Proteggere i dati personali e aziendali dalla compromissione dovuta al malware mediante strategie di difesa in profondità

4. Ruoli e responsabilità

4.1 Direttore generale (GM)

4.1.1 È il titolare della politica e assicura la disponibilità di risorse sufficienti per la protezione degli endpoint

4.1.2 Approva il software antivirus, gli strumenti di Mobile Device Management (MDM) e le regole di accesso da parte di terzi

4.1.3 Riesamina i report sugli incidenti malware, le sintesi di impatto e le notifiche di violazione che coinvolgono gli endpoint

4.2 Fornitore di supporto IT / Amministratore IT interno

4.2.1 Seleziona e distribuisce software antivirus, soluzioni antimalware ed Endpoint Detection and Response (EDR)

4.2.2 Garantisce che gli aggiornamenti siano applicati in modo coerente e che i log siano conservati

4.2.3 Risponde agli avvisi malware, isola i sistemi infetti e svolge le attività di rimedio

4.2.4 Applica i controlli sull'uso delle unità USB e dei dispositivi esterni

[... 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 Requisito di riesame annuale

9.1.1 La presente politica deve essere riesaminata formalmente almeno una volta all'anno dal Direttore generale, in coordinamento con il Fornitore di supporto IT e il Coordinatore privacy

9.2 Aggiornamenti attivati da eventi specifici

9.2.1 Gli aggiornamenti della politica devono avvenire anche quando:

9.2.1.1 Una nuova minaccia malware rilevante o un focolaio colpisce gli endpoint utilizzati dall'organizzazione

9.2.1.2 Gli strumenti antivirus o EDR vengono modificati, aggiornati o sostituiti

9.2.1.3 Un incidente malware evidenzia debolezze nell'ambito di applicazione o nell'attuazione della presente politica

9.2.1.4 Vengono aggiornati requisiti legali o regolamentari, ad esempio GDPR, DORA, NIS2

9.3 Controllo delle versioni e comunicazione

9.3.1 Tutte le modifiche alla politica devono essere documentate con numero di versione, data e sintesi delle modifiche

9.3.2 Il personale deve essere informato degli aggiornamenti, in particolare se modificano requisiti operativi o comportamentali

9.3.3 Le versioni precedenti devono essere conservate nell'archivio delle politiche per almeno 3 anni a supporto degli audit

10. Politiche correlate e collegamenti

10.1 La presente politica deve essere applicata congiuntamente alle seguenti politiche PMI:

10.1.1 P9S – Politica sul lavoro da remoto: garantisce che i requisiti di protezione degli endpoint siano applicati ai dispositivi utilizzati fuori sede o in modalità ibrida

10.1.2 P12S – Politica di gestione degli asset: supporta il tracciamento e il controllo di tutti gli endpoint, garantendo che siano utilizzati solo dispositivi autorizzati e protetti

10.1.3 P17S – Politica di protezione dei dati e privacy: rafforza la prevenzione del malware come controllo fondamentale per la tutela della privacy, al fine di proteggere dati personali e dati sensibili dalla compromissione

10.1.4 P22S – Politica di registrazione e monitoraggio: stabilisce i requisiti per la registrazione degli eventi malware e il mantenimento della visibilità delle allerte per una risposta tempestiva

10.1.5 P30S – Politica di risposta agli incidenti: definisce le fasi di escalation, contenimento e notifica esterna se il malware comporta compromissione dei dati o interruzione operativa

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 8.1 – Richiede l'implementazione di controlli operativi per ridurre rischi quali gli attacchi malware

11.2 ISO/IEC 27002

11.2.1 Controllo 8.7 – Descrive le pratiche di controllo del malware, inclusi antivirus, scansione in tempo reale, aggiornamenti e formazione degli utenti

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Richiede la distribuzione di meccanismi di protezione dal codice malevolo su tutti gli endpoint

11.3.2 SI-4 – Richiede attività di monitoraggio, rilevazione, analisi e risposta per minacce e allerte a livello di endpoint

11.4 Regolamento UE GDPR

11.4.1 Articolo 32(1)(b) – Richiede controlli tecnici e organizzativi, quali l'antivirus, per proteggere i dati personali

11.4.2 Articolo 33 – Impone la notifica della violazione dei dati personali quando il malware compromette integrità, riservatezza o disponibilità dei dati

11.5 Direttiva UE NIS2

11.5.1 Articolo 21(2)(d) – Richiede misure per prevenire e rispondere alle minacce malware all'interno dei soggetti essenziali e importanti

11.5.2 Articolo 21(2)(e) – Impone strategie di gestione del rischio di cibersicurezza a più livelli, inclusa la protezione degli endpoint dal malware

11.6 Regolamento UE DORA

11.6.1 Articolo 10(1) – Richiede che i sistemi ICT siano protetti dal malware e da altre minacce nell'ambito della resilienza operativa

11.6.2 Articolo 15 – Impone alle organizzazioni finanziarie di verificare la protezione dal malware presso i fornitori di servizi terzi

11.7 COBIT 2019

11.7.1 DSS05.02 – Sottolinea l'importanza di misure di protezione per difendere endpoint e reti dalle minacce malware

11.7.2 DSS05.04 – Supporta il monitoraggio e l'allerta sugli eventi di sicurezza correlati al malware nell'ambito delle operazioni continuative