					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P20					Dokumenttitel: **Politik for endepunktsbeskyttelse / malwarepolitik**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Endepunktsbeskyttelse og malwarebeskyttelse er påkrævet for at opfylde ISMS-mål
ISO/IEC 27002:2022	Kontroller 8.7, 8	Indeholder tekniske kontroller og vejledning om antimalware, endepunktsbeskyttelse og hændelseshåndtering
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definerer beskyttelse mod ondsindet kode, central overvågning og krav til baselinekonfiguration
EU GDPR	Artikel 32	Kræver passende tekniske foranstaltninger til beskyttelse af personoplysninger, herunder beskyttelse mod malware
EU NIS2	Artikel 21(2)(d)	Kræver implementering af trusselsdetektion på endepunktsniveau og forebyggende foranstaltninger
EU DORA	Artikel 9	Kræver styring af IKT-risici vedrørende malware og forsvar mod trusler, der kommer via endepunkter
COBIT 2019	DSS05.01, DSS01.04, MEA	Kræver beskyttelse, overvågning og vurdering af kontroller for endepunkter

1. Formål

1.1 Denne politik fastsætter de obligatoriske kontroller og driftsmæssige krav til beskyttelse af organisationens endepunkter, herunder stationære computere, bærbare computere, mobile enheder og servere, mod malware og relaterede trusler.

1.2 Den fastlægger minimumsstandarder for endepunktsbeskyttelse, malwaredetektion, inddæmningsrespons og adfærdsovervågning, så systemer forbliver robuste over for både udbredte og avancerede malwarevarianter.

1.3 Politikken understøtter direkte overholdelse af ISO/IEC 27001:2022 klausul 8.1 og bilag A-kontrol 8.7 og er tilpasset regionale cybersikkerhedsforpligtelser efter GDPR, NIS2 og DORA.

2. Omfang

2.1 Denne politik gælder for alle endepunkter, herunder:

2.1.1 Organisationsejede eller organisationsadministrerede stationære computere, bærbare computere, mobile enheder og virtuelle instanser

2.1.2 Private enheder godkendt efter BYOD-politikken, forudsat installation af MDM eller endepunktsagenter

2.1.3 Servere og infrastrukturaktiver, herunder cloud-hostede VM'er og edge-enheder

2.1.4 Operativsystemer, drivere, lokale tjenester, endepunktsagenter og sikkerhedskontroller installeret på hver node

2.2 Alle personer med administrativt, teknisk eller driftsmæssigt ansvar for et endepunkt er omfattet af denne politik, herunder:

2.2.1 Interne medarbejdere og kontrahenter

2.2.2 Managed service providers (MSP'er), outsourcet desktop-support og tredjeparts it-administratorer

2.2.3 Brugere, der er autoriseret til at anvende bærbare systemer, VPN-aktiverede bærbare computere eller mobil adgang til organisationens netværk

2.3 Trusselsdækningen under denne politik omfatter, men er ikke begrænset til:

2.3.1 Virus, orme, trojanske heste, ransomware, spyware, rootkits, adware, keyloggere og botnets

2.3.2 Filløs malware, zero-day-payloads, malware til privilegieeskalering og browserbaserede exploit kits

2.3.3 Ondsindet kode leveret via flytbare medier, phishingvektorer, drive-by-downloads eller USB-baserede angreb

3. Mål

3.1 Beskytte endepunktssystemers integritet, tilgængelighed og fortrolighed samt de data, de behandler, gennem pålidelig forebyggelse, detektion og håndtering af malware.

3.2 Forhindre eksekvering eller spredning af ondsindet kode på organisationens netværk ved at håndhæve tekniske sikkerhedsforanstaltninger, baselinehærdning og telemetri i realtid.

3.3 Integrere endepunktsbeskyttelse med øvrige ISMS-kontroller, herunder sårbarhedsstyring, adgangsstyring, logning og overvågning samt hændelseshåndtering.

3.4 Sikre løbende synlighed i endepunkter gennem centralt administrerede beskyttelsesplatforme, herunder antivirus-/antimalwareagenter, endpoint detection and response (EDR) og telemetri til SIEM-platforme.

3.5 Efterleve juridiske, regulatoriske og standardbaserede krav, der stiller krav til endepunktssikkerhed, herunder GDPR artikel 32, NIS2 artikel 21 og DORA artikel 9.

3.6 Definere ansvarlige roller, håndhæve SLA'er for patching og alarmrespons samt understøtte revisionsberedskab gennem dokumentation og rapportering.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer dens tilpasning til ISMS'et og den overordnede sikkerhedsstrategi.

4.1.2 Gennemgår kvartalsvist metrikker for endepunktsbeskyttelse, hændelsestendenser og værktøjernes effektivitet.

4.1.3 Godkender undtagelser og accept af restrisiko relateret til endepunktsdækning.

4.2 Endepunktssikkerhedsansvarlig / leder af Security Operations Center (SOC)

4.2.1 Administrerer systemer til endepunktsbeskyttelse, herunder AV, EDR og administration af mobile enheder (MDM).

4.2.2 Fører tilsyn med håndhævelse af politikken, finjustering af trusselsdetektion og respons-playbooks.

4.2.3 Vedligeholder dækningsstatistik, logfiler over malwarehændelser og baselinekonfigurationer for alarmer.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås årligt, eller når:

9.1.1 Der opstår større malwarekampagner eller sikkerhedshændelser vedrørende endepunkter

9.1.2 Nye trusselstyper, herunder filløs malware eller ransomwarevarianter, kræver opdaterede detektions- eller responsstrategier

9.1.3 Platforme til endepunktsbeskyttelse eller agentarkitekturer ændres væsentligt

9.1.4 Juridiske eller regulatoriske krav, der påvirker endepunktskontroller, opdateres

9.2 Gennemgangen skal iværksættes af den endepunktssikkerhedsansvarlige og koordineres med CISO, juridisk og compliance, risikostyringsfunktionen og revisionsfunktionen.

9.3 Godkendte ændringer skal dokumenteres i ISMS'ets dokumentstyringsregister, tildeles en ny versionsidentifikator og kommunikeres til alle berørte parter.

9.4 Erstattede versioner skal arkiveres, adgangsbegrænses og opbevares for at sikre revisionssporets integritet i overensstemmelse med ISMS'ets opbevaringsperioder.

10. Relaterede politikker og sammenhænge

10.1 P1 - Informationssikkerhedspolitik. Fastlægger grundlæggende principper for beskyttelse af systemer, data og netværk. Denne politik håndhæver disse principper på endepunktsniveau gennem tekniske og proceduremæssige malwarekontroller.

10.2 P4 - Politik for adgangskontrol. Definerer begrænsninger i brugeradgang, som håndhæves på endepunktslaget, herunder beskyttelse mod privilegieeskalering og uautoriserede installationer af ikkevurderet software.

10.3 P5 - Politik for ændringsstyring. Sikrer, at opdateringer til software til endepunktsbeskyttelse, politikregler eller agentkonfigurationer er underlagt godkendelse og kontrollerede udrulningsprocesser.

10.4 P12 - Politik for styring af aktiver. Giver den baseline for aktivklassificering og aktivfortegnelse, der er nødvendig for synlighed i endepunkter, patchdækning og afgrænsning af malwarebeskyttelsens omfang.

10.5 P22 - Lognings- og overvågningspolitik. Muliggør integration af alarmer fra endepunkter, agenters sundhedstilstand og trusselsintelligens i centraliserede SIEM-systemer til detektion i realtid og forensisk sporbarhed.

10.6 P30 - Politik for hændelseshåndtering. Knytter malwarehændelser på endepunkter til standardiserede arbejdsgange for inddæmning, fjernelse, undersøgelse og genopretning med tildelte roller og eskaleringstærskler.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:

11.1.1 Klausul 8.1 - operationel planlægning og styring: Kræver implementering af tekniske kontroller, herunder sikkerhedsforanstaltninger for endepunkter, for at opretholde ISMS-mål.

11.2 ISO/IEC 27002:2022 - kontroller 8.7, 8:

11.2.1 Indeholder detaljeret teknisk vejledning om antimalwareforanstaltninger, sikker udrulning af software, overvågning og hændelsesberedskab for endepunktsmiljøer.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Beskyttelse mod ondsindet kode: Kræver brug af antimalwareværktøjer med realtidsscanning, scanning ved adgang og adfærdsanalyse.

11.3.2 SI-4 - Systemovervågning: Understøtter integration af telemetri med centraliserede platforme til detektion.

11.3.3 CM-6 - Konfigurationsindstillinger: Understøtter baselinekontrolindstillinger på endepunkter, herunder håndhævelse af beskyttelsesagenter.

11.4 EU GDPR (2016/679):

11.4.1 Artikel 32 - behandlingssikkerhed: Kræver, at organisationer implementerer passende tekniske foranstaltninger til beskyttelse af personoplysninger, herunder beskyttelse mod malwaretrusler.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Artikel 21(2)(d): Forpligter enheder til at implementere foranstaltninger til trusselsdetektion og -forebyggelse, herunder mekanismer til malwarebeskyttelse på endepunktsniveau.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 9 - Krav til styring af IKT-risici: Kræver, at finansielle enheder indfører beskyttelsesforanstaltninger for at forebygge, detektere og håndtere malware og trusler, der kommer via endepunkter.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Beskyt mod malware: Kræver detektion og afbødning af malware på tværs af alle organisationens endepunkter.

11.7.2 DSS01.04 - Styr tilgængelighed og kapacitet: Sikrer, at malwarebeskyttelse afbalanceres med systemydelse og forretningskontinuitet.

11.7.3 MEA03 - Overvåg, evaluer og vurder overholdelse: Kræver periodisk revision af endepunktskontroller og beskyttelsens effektivitet.