					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P20					Documenttitel: **Endpointbescherming en malwarebeschermingbeleid**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	Endpointbeveiliging en malwarebescherming zijn vereist om de doelstellingen van het managementsysteem voor informatiebeveiliging (ISMS) te realiseren
ISO/IEC 27002:2022	Beheersmaatregelen 8.7, 8	Biedt technische beheersmaatregelen en richtlijnen voor antimalware, endpointbeveiliging en incidentbeheer
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definieert bescherming tegen schadelijke code, centrale monitoring en vereisten voor baselineconfiguratie
EU AVG	Artikel 32	Verplicht passende technische maatregelen ter bescherming van persoonsgegevens, waaronder bescherming tegen malware
EU NIS2	Artikel 21(2)(d)	Vereist de inzet van dreigingsdetectie en preventieve maatregelen op endpointniveau
EU DORA	Artikel 9	Vereist ICT-risicobeheer voor malware en bescherming tegen via endpoints overgedragen dreigingen
COBIT 2019	DSS05.01, DSS01.04, MEA	Verplicht bescherming, monitoring en beoordeling van endpointbeheersmaatregelen

1. Doel

1.1 Dit beleid definieert de verplichte beheersmaatregelen en operationele vereisten voor de bescherming van organisatorische endpoints, waaronder desktops, laptops, mobiele apparaten en servers, tegen malware en aanverwante dreigingen.

1.2 Het stelt minimumnormen vast voor endpointbeveiliging, malwaredetectie, indammingsrespons en gedragsmonitoring, zodat systemen weerbaar blijven tegen zowel gangbare als geavanceerde malwarevarianten.

1.3 Dit beleid ondersteunt rechtstreeks de naleving van ISO/IEC 27001:2022, clausule 8.1, en bijlage A, beheersmaatregel 8.7, en is afgestemd op regionale cyberbeveiligingsverplichtingen op grond van de AVG, NIS2 en DORA.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle endpoints, waaronder:

2.1.1 Desktops, laptops, mobiele apparaten en virtuele instanties die eigendom zijn van de organisatie of door de organisatie worden beheerd

2.1.2 Apparaten in persoonlijk eigendom die zijn toegestaan onder het Bring Your Own Device (BYOD)-beleid, mits MDM of endpointagents zijn geïnstalleerd

2.1.3 Servers en infrastructuuractiva, waaronder in de cloud gehoste VM's en edge-apparaten

2.1.4 Besturingssystemen, drivers, lokale services, endpointagents en beveiligingsmaatregelen die op iedere node zijn geïnstalleerd

2.2 Al het personeel met administratieve, technische of operationele verantwoordelijkheid voor enig endpoint valt onder dit beleid, waaronder:

2.2.1 Interne medewerkers en contractanten

2.2.2 Managed service providers (MSP's), uitbestede desktopondersteuning en IT-beheerders van derde partijen

2.2.3 Gebruikers die bevoegd zijn draagbare systemen, laptops met VPN-functionaliteit of mobiele toegang tot organisatienetwerken te gebruiken

2.3 De dreigingsdekking onder dit beleid omvat onder meer:

2.3.1 Virussen, wormen, trojans, ransomware, spyware, rootkits, adware, keyloggers en botnets

2.3.2 Bestandsloze malware, zero-day-payloads, malware voor privilege-escalatie en browser-exploitkits

2.3.3 Schadelijke code die wordt verspreid via verwisselbare media, phishingvectoren, drive-by-downloads of USB-gebaseerde aanvallen

3. Doelstellingen

3.1 De integriteit, beschikbaarheid en vertrouwelijkheid van endpointsystemen en de door deze systemen verwerkte gegevens beschermen door middel van robuuste malwarepreventie, detectie en respons.

3.2 De uitvoering of verspreiding van schadelijke code op organisatienetwerken voorkomen door technische beveiligingsmaatregelen, baselineconfiguratie en realtime telemetrie af te dwingen.

3.3 Endpointbeveiliging integreren met andere ISMS-beheersmaatregelen, waaronder kwetsbaarhedenbeheer, toegangsbeveiliging, logging en monitoring, en incidentrespons.

3.4 Continue zichtbaarheid van endpoints waarborgen met centraal beheerde beveiligingsplatforms, waaronder antivirus-/antimalwareagents, Endpoint Detection and Response (EDR) en SIEM-telemetrie.

3.5 Voldoen aan wettelijke, regelgevende en normatieve vereisten die endpointbeveiliging verplicht stellen, waaronder artikel 32 AVG, artikel 21 NIS2 en artikel 9 DORA.

3.6 Verantwoordelijkheden vastleggen, SLA's voor patching en respons op meldingen afdwingen en auditgereedheid ondersteunen via documentatie en rapportage.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en borgt de afstemming ervan op het ISMS en de overkoepelende beveiligingsstrategie.

4.1.2 Beoordeelt elk kwartaal endpointbeveiligingsmetingen, incidenttrends en de effectiviteit van hulpmiddelen.

4.1.3 Keurt uitzonderingen en acceptatie van restrisico met betrekking tot endpointdekking goed.

4.2 Verantwoordelijke Endpoint Security / SOC-manager

4.2.1 Beheert endpointbeveiligingssystemen, zoals AV, EDR en MDM.

4.2.2 Houdt toezicht op beleidshandhaving, afstemming van dreigingsdetectie en responsdraaiboeken.

4.2.3 Onderhoudt dekkingsstatistieken, logboeken van malware-incidenten en baselineconfiguraties voor waarschuwingen.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisering

9.1 Dit beleid moet jaarlijks worden herzien of wanneer:

9.1.1 Er grootschalige malwarecampagnes of endpointbeveiligingsincidenten plaatsvinden

9.1.2 Nieuwe dreigingstypen, zoals bestandsloze malware of ransomwarevarianten, geactualiseerde detectie- of responsstrategieën vereisen

9.1.3 Endpointbeveiligingsplatforms of agentarchitecturen ingrijpend wijzigen

9.1.4 Wettelijke of regelgevende vereisten die endpointbeheersmaatregelen beïnvloeden, worden bijgewerkt

9.2 De herziening wordt geïnitieerd door de verantwoordelijke voor Endpoint Security en gecoördineerd met de CISO en de functies Juridische Zaken, Risk en Audit.

9.3 Goedgekeurde herzieningen moeten worden gedocumenteerd in het ISMS-documentregister, van een nieuwe versie-identificatie worden voorzien en aan alle betrokken partijen worden gecommuniceerd.

9.4 Vervangen versies moeten worden gearchiveerd, in toegang worden beperkt en conform de ISMS-bewaartermijnen worden bewaard ter borging van de integriteit van de audittrail.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 P1 - Informatiebeveiligingsbeleid. Stelt de basisprincipes vast voor de bescherming van systemen, gegevens en netwerken. Dit beleid operationaliseert die principes op endpointniveau via technische en procedurele malwarebeheersmaatregelen.

10.2 P4 - Beleid inzake toegangsbeveiliging. Definieert beperkingen op gebruikerstoegang die op endpointniveau worden afgedwongen, waaronder bescherming tegen privilege-escalatie en ongeautoriseerde installatie van niet-beoordeelde software.

10.3 P5 - Wijzigingsbeheerbeleid. Borgt dat updates van endpointbeveiligingssoftware, beleidsregels of agentconfiguraties onderworpen zijn aan goedkeuring en gecontroleerde uitrolprocessen.

10.4 P12 - Beleid inzake bedrijfsmiddelenbeheer. Biedt de basis voor classificatie van bedrijfsmiddelen en de inventaris die nodig is voor zichtbaarheid van endpoints, patchdekking en afbakening van de reikwijdte van malwarebescherming.

10.5 P22 - Logging- en monitoringbeleid. Maakt integratie mogelijk van endpointwaarschuwingen, de status van agents en threat intelligence in gecentraliseerde SIEM-systemen voor realtime detectie en forensische traceerbaarheid.

10.6 P30 - Incidentresponsbeleid (P30). Verbindt malware-incidenten op endpointniveau met gestandaardiseerde werkstromen voor indamming, uitroeiing, onderzoek en herstel, inclusief toegewezen rollen en escalatiedrempels.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001:

11.1.1 Clausule 8.1 - Operationele planning en beheersing: vereist de implementatie van technische beheersmaatregelen, waaronder endpointbeveiliging, om de doelstellingen van het ISMS te borgen.

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

11.2.1 Biedt gedetailleerde technische richtlijnen voor antimalwaremaatregelen, veilige uitrol van software, monitoring en incidentparaatheid in endpointomgevingen.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Bescherming tegen schadelijke code: vereist het gebruik van antimalwaretools met realtime scanning bij toegang en gedragsanalyse.

11.3.2 SI-4 - Systeemmonitoring: ondersteunt integratie van telemetrie met gecentraliseerde detectieplatforms.

11.3.3 CM-6 - Configuratie-instellingen: versterkt baseline-instellingen op endpoints, waaronder afdwinging van beschermingsagents.

11.4 EU AVG (2016/679):

11.4.1 Artikel 32 - Beveiliging van de verwerking: vereist dat organisaties passende technische maatregelen implementeren ter bescherming van persoonsgegevens, waaronder bescherming tegen malwaredreigingen.

11.5 EU NIS2-richtlijn (2022/2555):

11.5.1 Artikel 21(2)(d): verplicht entiteiten om maatregelen voor dreigingsdetectie en -preventie in te zetten, waaronder malwarebeschermingsmechanismen op endpointniveau.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 9 - Vereisten inzake ICT-risicobeheer: vereist dat financiële entiteiten beschermende maatregelen treffen om malware en via endpoints overgedragen dreigingen te voorkomen, te detecteren en erop te reageren.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Bescherming tegen malware: verplicht detectie en mitigatie van malware op alle organisatorische endpoints.

11.7.2 DSS01.04 - Beschikbaarheid en capaciteit beheren: borgt dat malwarebescherming in balans is met systeemprestaties en bedrijfscontinuïteit.

11.7.3 MEA03 - Monitoren, evalueren en beoordelen van naleving: vereist periodieke audit van endpointbeheersmaatregelen en de effectiviteit van de bescherming.