					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P20S					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	Operationele beheersmaatregelen voor malwarebescherming
ISO/IEC 27002:2022	Beheersmaatregel 8	Beheersmaatregelen voor endpointbeveiliging
NIST SP 800-53 Rev.5	SI-3, SI-4	Bescherming tegen kwaadaardige code en incidentrespons
EU NIS2	Artikelen 21(2)(d), (e)	Malware en risicobeheer voor essentiële/belangrijke entiteiten
EU DORA	Artikelen 10(1), 15	Operationele weerbaarheid en verificatie van derde partijen
COBIT 2019	DSS05.02, DSS05.04	Endpoint- en netwerkbeveiliging en monitoring
AVG	Artikelen 32(1)(b), 33	Technische en organisatorische maatregelen en meldplicht bij inbreuken

1. Doel

1.1 Dit beleid definieert de minimale technische, procedurele en gedragsmatige vereisten voor de bescherming van alle endpointapparaten, zoals laptops, desktops, mobiele apparaten en draagbare media, tegen kwaadaardige code, waaronder virussen, ransomware, spyware, rootkits en andere malwaredreigingen.

1.2 Het doel is te waarborgen dat endpoints zodanig worden ingericht, beheerd en gebruikt dat het risico op malware-infectie, verspreiding en systeemcompromittering wordt beperkt.

1.3 De organisatie erkent dat endpoints veelvoorkomende toegangspunten voor malware zijn en daarom moeten worden gehard, bewaakt en beschermd met meerdere verdedigingslagen.

1.4 Dit beleid ondersteunt de certificeringsdoelstellingen van de organisatie onder ISO/IEC 27001:2022 en is afgestemd op de Algemene Verordening Gegevensbescherming (AVG), de NIS2-richtlijn, de Digital Operational Resilience Act (DORA) en andere relevante raamwerken.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle endpoints van de organisatie, waaronder desktops, laptops, tablets, mobiele telefoons en point-of-sale-terminals

2.1.2 persoonlijk eigendom zijnde Bring Your Own Device (BYOD)-apparaten die worden gebruikt voor toegang tot bedrijfstoepassingen of gegevens

2.1.3 verwijderbare opslagmedia, zoals USB-sticks en externe harde schijven

2.1.4 alle besturingssystemen, endpointsoftware en communicatiemiddelen die op deze platforms draaien

2.2 Dit beleid geldt in gelijke mate voor:

2.2.1 interne medewerkers, contractanten, stagiairs en managed service providers (MSP's)

2.2.2 apparaten die op locatie, op afstand of binnen hybride werkregelingen worden gebruikt

2.2.3 cloudverbonden of offline endpoints waarop bedrijfsgegevens of persoonsgegevens worden opgeslagen

3. Doelstellingen

3.1 Het voorkomen van malware-infecties en -verspreiding binnen interne systemen, gebruikersapparaten en externe verbindingen

3.2 Malwaregerelateerde dreigingen snel detecteren en indammen met geautomatiseerde endpointbeveiligingstools en vastgestelde escalatieprocedures

3.3 Waarborgen dat uitsluitend geautoriseerde, beveiligde en bewaakte apparaten worden gebruikt voor toegang tot bedrijfsinformatie

3.4 Duidelijke verantwoordelijkheden en bindende gedragsregels voor medewerkers vaststellen om het risico op malwaregerelateerde incidenten te beperken

3.5 Traceerbare en auditeerbare registraties van malwaredetecties, responsacties en naleving van beleid bijhouden

3.6 Persoonsgegevens en bedrijfsgegevens beschermen tegen compromittering door malware met meerlaagse verdedigingsstrategieën

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur

4.1.1 is eigenaar van dit beleid en ziet erop toe dat voldoende middelen beschikbaar zijn voor endpointbeveiliging

4.1.2 keurt antivirussoftware, oplossingen voor mobielapparaatbeheer (MDM) en regels voor toegang door derden goed

4.1.3 beoordeelt rapportages over malware-incidenten, impactsamenvattingen en meldingen van inbreuken waarbij endpoints betrokken zijn

4.2 IT-supportdienstverlener / interne IT-beheerder

4.2.1 selecteert en implementeert antivirus-, antimalware- en Endpoint Detection and Response (EDR)-software

4.2.2 ziet erop toe dat updates consistent worden toegepast en logbestanden worden bewaard

4.2.3 reageert op malwaremeldingen, isoleert geïnfecteerde systemen en voert herstelmaatregelen uit

4.2.4 handhaaft beheersmaatregelen voor het gebruik van USB-apparaten en externe apparatuur

[... 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 bijwerking

9.1 Jaarlijkse beoordelingsvereiste

9.1.1 Dit beleid moet ten minste eenmaal per jaar formeel worden beoordeeld door de algemeen directeur, in afstemming met de IT-supportdienstverlener en de privacycoördinator

9.2 Updates op basis van triggers

9.2.1 Beleidsupdates moeten ook plaatsvinden wanneer:

9.2.1.1 een nieuwe majeure malwaredreiging of uitbraak gericht is op endpoints die door de organisatie worden gebruikt

9.2.1.2 antivirus- of EDR-tools worden gewijzigd, geüpgraded of vervangen

9.2.1.3 een malware-incident zwakke punten in de reikwijdte of handhaving van dit beleid blootlegt

9.2.1.4 wettelijke of regelgevende vereisten (bijvoorbeeld AVG, DORA, NIS2) worden bijgewerkt

9.3 Versiebeheer en communicatie

9.3.1 Alle beleidswijzigingen moeten worden gedocumenteerd met een versienummer, datum en samenvatting van wijzigingen

9.3.2 Medewerkers moeten over updates worden geïnformeerd, vooral als deze operationele of gedragsmatige vereisten wijzigen

9.3.3 Eerdere versies moeten ten minste 3 jaar in het beleidsarchief worden bewaard ter ondersteuning van audits

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid moet worden geïmplementeerd in samenhang met de volgende mkb-beleidsdocumenten:

10.1.1 P9S – Beleid voor werken op afstand: waarborgt dat vereisten voor endpointbeveiliging worden gehandhaafd op apparaten die buiten de locatie of in hybride omgevingen worden gebruikt

10.1.2 P12S – Beleid voor bedrijfsmiddelenbeheer: ondersteunt het volgen en beheersen van alle endpoints en waarborgt dat uitsluitend geautoriseerde en beschermde apparaten worden gebruikt

10.1.3 P17S – Beleid voor gegevensbescherming en privacy: versterkt malwarepreventie als kernmaatregel ter bescherming van persoonsgegevens en gevoelige gegevens tegen compromittering

10.1.4 P22S – Beleid voor logging en monitoring: stelt de vereisten vast voor het loggen van malwaregebeurtenissen en het behouden van zichtbaarheid op waarschuwingen voor tijdige respons

10.1.5 P30S – Incidentresponsbeleid: definieert escalatie-, indammings- en externe meldstappen indien malware leidt tot datacompromittering of operationele verstoring

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – vereist de implementatie van operationele beheersmaatregelen om risico's zoals malwareaanvallen te beperken

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.7 – beschrijft beheerspraktijken voor malware, waaronder antivirus, realtime scanning, updates en gebruikerstraining

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – vereist de uitrol van beschermingsmechanismen tegen kwaadaardige code op endpoints

11.3.2 SI-4 – schrijft monitoring-, detectie-, analyse- en responsacties voor voor dreigingen en waarschuwingen op endpointniveau

11.4 AVG

11.4.1 Artikel 32(1)(b) – vereist technische en organisatorische beheersmaatregelen (zoals antivirus) ter bescherming van persoonsgegevens

11.4.2 Artikel 33 – verplicht melding van een inbreuk wanneer malware de integriteit, vertrouwelijkheid of beschikbaarheid van gegevens compromitteert

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(d) – vereist maatregelen om malwaredreigingen binnen essentiële en belangrijke entiteiten te voorkomen en erop te reageren

11.5.2 Artikel 21(2)(e) – schrijft gelaagde strategieën voor cyberbeveiligingsrisicobeheer voor, waaronder bescherming van endpoints tegen malware

11.6 EU DORA

11.6.1 Artikel 10(1) – vereist dat ICT-systemen worden beschermd tegen malware en andere dreigingen als onderdeel van operationele weerbaarheid

11.6.2 Artikel 15 – verplicht financiële organisaties de malwarebescherming bij externe ICT-dienstverleners te verifiëren

11.7 COBIT 2019

11.7.1 DSS05.02 – benadrukt beschermende maatregelen om endpoints en netwerken tegen malwaredreigingen te beveiligen

11.7.2 DSS05.04 – ondersteunt het monitoren van en waarschuwen voor malwaregerelateerde beveiligingsgebeurtenissen als onderdeel van de doorlopende operatie