					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P20S					Dokumenttitel: **Politik for malwarebeskyttelse af endepunkter**							
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	Operationelle kontroller for malwarebeskyttelse
ISO/IEC 27002:2022	Kontrol 8	Kontroller for beskyttelse af endepunkter
NIST SP 800-53 Rev.5	SI-3, SI-4	Beskyttelse mod ondsindet kode og hændelseshåndtering
EU NIS2	Artikel 21(2)(d), (e)	Malware og risikostyring for væsentlige og vigtige enheder
EU DORA	Artikel 10(1), 15	Operationel robusthed og verifikation af tredjeparter
COBIT 2019	DSS05.02, DSS05.04	Beskyttelse og overvågning af endepunkter/netværk
EU GDPR	Artikel 32(1)(b), 33	Tekniske og organisatoriske foranstaltninger samt underretning om brud

1. Formål

1.1 Denne politik fastsætter de minimumskrav af teknisk, proceduremæssig og adfærdsmæssig karakter, der gælder for beskyttelse af alle brugerendepunkter – såsom bærbare computere, stationære computere, mobile enheder og flytbare medier – mod ondsindet kode, herunder virus, ransomware, spyware, rootkits og andre malwaretrusler.

1.2 Formålet er at sikre, at endepunkter er udstyret, vedligeholdt og anvendt på en måde, der reducerer risikoen for malwareinfektion, spredning og kompromittering af systemer.

1.3 Organisationen anerkender, at endepunkter er almindelige indgangspunkter for malware og derfor skal være hærdede, overvågede og beskyttede ved anvendelse af flere forsvarslag.

1.4 Politikken understøtter organisationens certificeringsmål efter ISO/IEC 27001:2022 og er tilpasset databeskyttelsesforordningen (GDPR), NIS2-direktivet, forordningen om digital operationel modstandsdygtighed (DORA) og andre relevante rammeværker.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle organisationens endepunkter, herunder stationære computere, bærbare computere, tablets, mobiltelefoner og point-of-sale-terminaler

2.1.2 Private enheder (BYOD), der anvendes til adgang til forretningsapplikationer eller data

2.1.3 Flytbare lagringsenheder såsom USB-drev og eksterne harddiske

2.1.4 Alle operativsystemer, endpoint-software eller kommunikationsværktøjer, der kører på disse platforme

2.2 Den gælder tilsvarende for:

2.2.1 Interne medarbejdere, kontraktansatte, tredjepartsleverandører, praktikanter og managed service providers (MSP'er)

2.2.2 Enheder, der anvendes on-site, ved fjernarbejde eller i hybride arbejdsformer

2.2.3 Cloudforbundne eller offline endepunkter, der lagrer forretningsdata eller personoplysninger

3. Mål

3.1 Forebygge malwareinfektion og spredning på tværs af interne systemer, brugerenheder og eksterne forbindelser

3.2 Detektere og inddæmme malwarerelaterede trusler hurtigt ved hjælp af automatiserede teknologier til endepunktssikkerhed og definerede eskalationsveje

3.3 Sikre, at kun godkendte, sikrede og overvågede enheder anvendes til adgang til forretningsoplysninger

3.4 Håndhæve klare ansvarsforhold og adfærdsregler for brugere for at reducere risikoen for malwarerelaterede hændelser

3.5 Opretholde sporbare og revisionsklare registreringer af malwaredetektioner, respons og efterlevelse af politikken

3.6 Beskytte personoplysninger og forretningsdata mod kompromittering som følge af malware ved anvendelse af lagdelte forsvarsstrategier

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Er ansvarlig for denne politik og sikrer, at der er tilstrækkelige ressourcer til beskyttelse af endepunkter

4.1.2 Godkender antivirussoftware, værktøjer til styring af mobile enheder (MDM) og regler for adgang for tredjeparter

4.1.3 Gennemgår rapporter om malwarehændelser, konsekvensvurderinger og underretninger om brud, der involverer endepunkter

4.2 IT-supportleverandør / intern it-administrator

4.2.1 Udvælger og implementerer antivirus-, antimalware- og endpoint detection and response (EDR)-software

4.2.2 Sikrer, at opdateringer gennemføres konsekvent, og at logfiler opbevares

4.2.3 Reagerer på malwarealarmer, isolerer inficerede systemer og gennemfører afhjælpning

4.2.4 Håndhæver kontroller for brug af USB-enheder og eksterne enheder

[... 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 Krav om årlig gennemgang

9.1.1 Denne politik skal gennemgås formelt mindst én gang om året af direktøren i koordinering med IT-supportleverandøren og databeskyttelseskoordinatoren

9.2 Opdateringer udløst af hændelser

9.2.1 Politikken skal også opdateres, når:

9.2.1.1 En væsentlig ny malwaretrussel eller et udbrud retter sig mod endepunkter, som organisationen anvender

9.2.1.2 Antivirus- eller EDR-værktøjer ændres, opgraderes eller udskiftes

9.2.1.3 En malwarehændelse afslører svagheder i denne politiks omfang eller håndhævelse

9.2.1.4 Lovgivningsmæssige eller regulatoriske krav (f.eks. GDPR, DORA, NIS2) opdateres

9.3 Versionsstyring og kommunikation

9.3.1 Alle ændringer i politikken skal dokumenteres med versionsnummer, dato og et resumé af ændringerne

9.3.2 Medarbejdere skal underrettes om opdateringer, især hvis de ændrer operationelle krav eller adfærdskrav

9.3.3 Tidligere versioner skal opbevares i politikarkivet i mindst 3 år for at understøtte revisioner

10. Relaterede politikker og sammenhænge

10.1 Denne politik skal implementeres sammen med følgende SME-politikker:

10.1.1 P9S – Politik for fjernarbejde: Sikrer, at krav til beskyttelse af endepunkter håndhæves på enheder, der anvendes uden for organisationens lokationer eller i hybride arbejdsformer

10.1.2 P12S – Politik for styring af aktiver: Understøtter sporing og kontrol af alle endepunkter og sikrer, at kun godkendte og beskyttede enheder anvendes

10.1.3 P17S – Databeskyttelses- og privatlivspolitik: Understreger malwareforebyggelse som en central privatlivskontrol til beskyttelse af personoplysninger og følsomme data mod kompromittering

10.1.4 P22S – Lognings- og overvågningspolitik: Fastlægger krav til logning af malwarehændelser og opretholdelse af synlighed i alarmer med henblik på tidlig respons

10.1.5 P30S – Politik for hændelseshåndtering: Definerer eskalation, inddæmning og ekstern underretning, hvis malware medfører kompromittering af data eller driftsforstyrrelser

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kræver implementering af operationelle kontroller for at reducere risici såsom malwareangreb

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.7 – Beskriver praksis for malwarekontrol, herunder antivirus, realtidsscanning, opdateringer og brugertræning

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Kræver implementering af mekanismer til beskyttelse mod ondsindet kode på tværs af endepunkter

11.3.2 SI-4 – Kræver overvågning, detektion, analyse og respons for trusler og alarmer på endepunktsniveau

11.4 EU GDPR

11.4.1 Artikel 32(1)(b) – Kræver tekniske og organisatoriske kontroller (såsom antivirus) til beskyttelse af personoplysninger

11.4.2 Artikel 33 – Forpligter til underretning om brud, når malware kompromitterer dataintegritet, fortrolighed eller tilgængelighed

11.5 EU NIS2-direktiv

11.5.1 Artikel 21(2)(d) – Kræver foranstaltninger til at forebygge og reagere på malwaretrusler i væsentlige og vigtige enheder

11.5.2 Artikel 21(2)(e) – Kræver lagdelte strategier for styring af cybersikkerhedsrisici, herunder malwarebeskyttelse af endepunkter

11.6 EU DORA

11.6.1 Artikel 10(1) – Kræver, at IKT-systemer beskyttes mod malware og andre trusler som led i operationel robusthed

11.6.2 Artikel 15 – Forpligter finansielle organisationer til at verificere malwarebeskyttelse hos tredjepartsleverandører

11.7 COBIT 2019

11.7.1 DSS05.02 – Fremhæver beskyttelsesforanstaltninger til forsvar af endepunkter og netværk mod malwaretrusler

11.7.2 DSS05.04 – Understøtter overvågning og alarmering ved malwarerelaterede sikkerhedshændelser som led i den løbende drift