					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P20S					Dokumenttitel: **Endpointskyddspolicy – skadlig kod**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Operativa kontroller för skydd mot skadlig kod
ISO/IEC 27002:2022	Kontroll 8	Kontrollåtgärder för endpointskydd
NIST SP 800-53 Rev.5	SI-3, SI-4	Skydd mot skadlig kod och incidenthantering
EU:s NIS2-direktiv	Artiklarna 21.2 d, e	Skydd mot skadlig kod och riskhantering för väsentliga och viktiga entiteter
EU:s DORA-förordning	Artiklarna 10.1, 15	Operativ resiliens och verifiering av tredjepart
COBIT 2019	DSS05.02, DSS05.04	Skydd av slutpunkter och nätverk samt övervakning
EU:s GDPR	Artiklarna 32.1 b, 33	Tekniska och organisatoriska åtgärder samt anmälan av personuppgiftsincident

1. Syfte

1.1 Denna policy fastställer de lägsta tekniska, processuella och beteendemässiga kraven för att skydda alla slutpunkter – såsom bärbara datorer, stationära datorer, mobila enheter och flyttbara lagringsmedier – mot skadlig kod, inklusive virus, ransomware, spionprogram, rootkits och andra hot.

1.2 Syftet är att säkerställa att slutpunkter är utrustade, underhållna och används på ett sätt som minskar risken för infektion, spridning av skadlig kod och kompromettering av system.

1.3 Organisationen konstaterar att slutpunkter är vanliga angreppspunkter för skadlig kod och ska därför vara härdade, övervakade och skyddade genom försvar i djupled.

1.4 Policyn stödjer organisationens certifieringsmål enligt ISO/IEC 27001:2022 och är anpassad till EU:s GDPR, EU:s NIS2-direktiv, EU:s DORA-förordning och andra relevanta ramverk.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Samtliga av organisationens slutpunkter, inklusive stationära datorer, bärbara datorer, surfplattor, mobiltelefoner och kassasystem

2.1.2 Privatägda enheter (BYOD) som används för åtkomst till verksamhetsapplikationer eller data

2.1.3 Flyttbara lagringsmedier såsom USB-minnen och externa hårddiskar

2.1.4 Operativsystem, endpointprogramvara och kommunikationsverktyg som körs på dessa plattformar

2.2 Policyn gäller i lika hög grad för:

2.2.1 Intern personal, entreprenörer, tredjepartstjänsteleverantörer, praktikanter och leverantörer av hanterade tjänster

2.2.2 Enheter som används i organisationens lokaler, på distans eller inom ramen för hybridarbete

2.2.3 Slutpunkter i molnmiljö eller offline som lagrar verksamhetsinformation eller personuppgifter

3. Mål

3.1 Förebygga infektion och spridning av skadlig kod i interna system, användarenheter och externa anslutningar

3.2 Upptäcka och begränsa hot relaterade till skadlig kod snabbt med hjälp av automatiserade verktyg för endpointskydd och fastställda eskaleringsvägar

3.3 Säkerställa att endast behöriga, skyddade och övervakade enheter används för åtkomst till verksamhetsinformation

3.4 Säkerställa tydligt ansvar för personalen och tydliga beteenderegler för användare för att minska risken för incidenter relaterade till skadlig kod

3.5 Upprätthålla spårbara och verifierbara underlag för detektering av skadlig kod, åtgärder och efterlevnad av policyn

3.6 Skydda personuppgifter och verksamhetsinformation mot kompromettering till följd av skadlig kod genom försvar i djupled

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 Är policyägare för denna policy och säkerställer att tillräckliga resurser finns tillgängliga för endpointskydd

4.1.2 Godkänner antivirusprogramvara, lösningar för hantering av mobila enheter och regler för tredjepartsåtkomst

4.1.3 Granskar incidentrapporter om skadlig kod, konsekvenssammanfattningar och avvikelserapporter som rör slutpunkter

4.2 IT-supportleverantör / intern IT-administratör

4.2.1 Väljer och inför antivirus, lösningar mot skadlig kod samt endpoint detection and response (EDR)

4.2.2 Säkerställer att uppdateringar tillämpas konsekvent och att loggar bevaras

4.2.3 Hanterar larm om skadlig kod, isolerar infekterade system och genomför korrigerande åtgärder

4.2.4 Säkerställer kontroller för användning av USB-enheter och externa enheter

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Krav på årlig granskning

9.1.1 Denna policy ska granskas formellt minst en gång per år av verkställande direktör i samordning med IT-supportleverantören och integritetssamordnaren

9.2 Uppdateringar vid utlösande händelser

9.2.1 Policyn ska också uppdateras när:

9.2.1.1 Ett nytt större hot eller utbrott av skadlig kod riktas mot de slutpunkter som används av organisationen

9.2.1.2 Verktyg för antivirus eller EDR ändras, uppgraderas eller ersätts

9.2.1.3 En incident med skadlig kod visar på svagheter i policyomfattningen eller tillämpningen av denna policy

9.2.1.4 Rättsliga eller regulatoriska krav, till exempel EU:s GDPR, EU:s DORA-förordning eller EU:s NIS2-direktiv, uppdateras

9.3 Versionshantering och kommunikation

9.3.1 Alla policyändringar ska dokumenteras med versionsnummer, datum och ändringssammanfattning

9.3.2 Personalen ska informeras om uppdateringar, särskilt om de ändrar operativa krav eller beteendekrav

9.3.3 Tidigare versioner ska bevaras i policyarkivet i minst 3 år för att stödja revisioner

10. Relaterade policyer och kopplingar

10.1 Denna policy ska genomföras tillsammans med följande SME-policyer:

10.1.1 P9S – Policy för distansarbete: Säkerställer att krav på endpointskydd tillämpas på enheter som används utanför arbetsplatsen eller i hybridmiljöer

10.1.2 P12S – Policy för tillgångshantering: Stödjer spårning och kontroll av alla slutpunkter så att endast behöriga och skyddade enheter används

10.1.3 P17S – Policy för dataskydd och integritet: Förstärker förebyggande skydd mot skadlig kod som en central integritetskontroll för att skydda personuppgifter och känsliga data mot kompromettering

10.1.4 P22S – Loggnings- och övervakningspolicy: Fastställer krav för loggning av händelser relaterade till skadlig kod och bibehållen synlighet i larm för tidig hantering

10.1.5 P30S – Policy för incidenthantering: Definierar eskalering, begränsning och externa anmälningar om skadlig kod leder till datakompromettering eller operativ störning

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver införande av operativa kontroller för att minska risker såsom angrepp med skadlig kod

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.7 – Beskriver praxis för kontroll av skadlig kod, inklusive antivirus, realtidsskanning, uppdateringar och användarutbildning

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Kräver införande av skyddsmekanismer mot skadlig kod på slutpunkter

11.3.2 SI-4 – Kräver övervakning, detektering, analys och åtgärder för hot och larm på slutpunktsnivå

11.4 EU:s GDPR

11.4.1 Artikel 32.1 b – Kräver tekniska och organisatoriska kontroller, såsom antivirus, för att skydda personuppgifter

11.4.2 Artikel 33 – Kräver anmälan av personuppgiftsincident när skadlig kod komprometterar riktighet, konfidentialitet eller tillgänglighet för data

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21.2 d – Kräver åtgärder för att förebygga och hantera hot från skadlig kod inom väsentliga och viktiga entiteter

11.5.2 Artikel 21.2 e – Kräver lagerindelade strategier för cybersäkerhetsriskhantering, inklusive skydd mot skadlig kod på slutpunkter

11.6 EU:s DORA-förordning

11.6.1 Artikel 10.1 – Kräver att IKT-system skyddas mot skadlig kod och andra hot som en del av operativ resiliens

11.6.2 Artikel 15 – Kräver att finansiella organisationer verifierar skydd mot skadlig kod hos tredjepartstjänsteleverantörer

11.7 COBIT 2019

11.7.1 DSS05.02 – Betonar skyddsåtgärder för att försvara slutpunkter och nätverk mot hot från skadlig kod

11.7.2 DSS05.04 – Stödjer övervakning och larmning av malware-relaterade säkerhetshändelser som en del av den löpande driften