					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P20					Dokumenttitel: **Policy för endpointskydd och skydd mot 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**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Endpointskydd och skydd mot skadlig kod krävs för att uppnå målen för ledningssystemet för informationssäkerhet
ISO/IEC 27002:2022	Kontroller 8.7, 8	Tillhandahåller tekniska kontroller och vägledning för skydd mot skadlig kod, endpointskydd och incidenthantering
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definierar skydd mot skadlig kod, centraliserad övervakning och krav på säker baskonfiguration
EU:s GDPR	Artikel 32	Kräver lämpliga tekniska åtgärder för att skydda personuppgifter, inklusive skydd mot skadlig kod
EU:s NIS2-direktiv	Artikel 21(2)(d)	Kräver införande av hotdetektering och förebyggande åtgärder på endpointnivå
EU:s DORA-förordning	Artikel 9	Kräver IKT-riskhantering avseende skadlig kod och skydd mot endpointrelaterade hot
COBIT 2019	DSS05.01, DSS01.04, MEA03	Kräver skydd, övervakning och bedömning av endpointkontroller

1. Syfte

1.1 Denna policy definierar de obligatoriska kontrollerna och operativa kraven för att skydda organisationens endpoints, inklusive stationära datorer, bärbara datorer, mobila enheter och servrar, mot skadlig kod och relaterade hot.

1.2 Den fastställer minimikrav för endpointskydd, detektering av skadlig kod, begränsningsåtgärder och beteendeövervakning för att säkerställa att systemen förblir motståndskraftiga mot både vanligt förekommande och avancerade varianter av skadlig kod.

1.3 Policyn stöder direkt efterlevnad av ISO/IEC 27001:2022 klausul 8.1 och bilaga A, kontroll 8.7, samt är anpassad till regionala cybersäkerhetskrav enligt GDPR, NIS2 och DORA.

2. Omfattning

2.1 Denna policy gäller för alla endpoints, inklusive:

2.1.1 Organisationens ägda eller förvaltade stationära datorer, bärbara datorer, mobila enheter och virtuella instanser

2.1.2 Privatägda enheter som är godkända enligt policyn för Bring Your Own Device (BYOD), under förutsättning att MDM eller agenter för endpointsäkerhet är installerade

2.1.3 Servrar och infrastrukturtillgångar, inklusive virtuella maskiner i molnmiljöer och edge-enheter

2.1.4 Operativsystem, drivrutiner, lokala tjänster, agenter för endpointsäkerhet och säkerhetskontroller som är installerade på varje nod

2.2 All personal med administrativt, tekniskt eller operativt ansvar för någon endpoint omfattas av denna policy, inklusive:

2.2.1 Interna anställda, konsulter och tredjepartsleverantörer

2.2.2 Managed Service Providers (MSP), outsourcad desktopsupport och tredjepartsadministratörer inom IT

2.2.3 Användare som är behöriga att använda portabla system, bärbara datorer med VPN eller mobil åtkomst till organisationens nätverk

2.3 Hot som omfattas av denna policy inkluderar, men är inte begränsade till:

2.3.1 Virus, maskar, trojaner, ransomware, spionprogram, rootkits, annonsprogram, keyloggers och botnät

2.3.2 Fillös skadlig kod, zero day-laster, skadlig kod för privilegieeskalering och exploit kits för webbläsare

2.3.3 Skadlig kod som levereras via flyttbara lagringsmedier, phishingvektorer, drive-by-nedladdningar eller USB-baserade attacker

3. Mål

3.1 Skydda riktighet, tillgänglighet och konfidentialitet i endpointsystem och de data de behandlar genom tillförlitligt förebyggande skydd, detektering och hantering av skadlig kod.

3.2 Förhindra exekvering eller spridning av skadlig kod i organisationens nätverk genom att tillämpa tekniska skyddsåtgärder, säker baskonfiguration och telemetri i realtid.

3.3 Integrera endpointskydd med andra ISMS-kontroller, inklusive sårbarhetshantering, åtkomstkontroll, loggning och övervakning samt incidenthantering.

3.4 Säkerställa kontinuerlig synlighet för endpoints genom centralt hanterade skyddsplattformar, inklusive antiviruslösningar/lösningar mot skadlig kod, Endpoint Detection and Response (EDR) samt SIEM-telemetri.

3.5 Uppfylla rättsliga, regulatoriska och standardbaserade krav som ställer krav på endpointsäkerhet, till exempel artikel 32 i GDPR, artikel 21 i NIS2 och artikel 9 i DORA.

3.6 Definiera ansvariga roller, tillämpa SLA:er för patchning och larmhantering samt säkerställa revisionsberedskap genom dokumentation, revisionsspår och rapportering.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Är policyägare för denna policy och säkerställer att den är anpassad till ISMS och den övergripande säkerhetsstrategin.

4.1.2 Granskar kvartalsvis nyckeltal för endpointskydd, incidenttrender och verktygens effektivitet.

4.1.3 Godkänner undantag och acceptans av restrisk relaterad till täckning av endpoints.

4.2 Ansvarig för endpointskydd / chef för Security Operations Center (SOC)

4.2.1 Förvaltar system för endpointskydd, till exempel antivirus, EDR och hantering av mobila enheter.

4.2.2 Ansvarar för efterlevnad av policyn, finjustering av hotdetektering och operativa åtgärdsplaner för hantering.

4.2.3 Upprätthåller statistik över täckning, incidentloggar för skadlig kod och säker baskonfiguration för larm.

[... 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 Denna policy ska granskas årligen eller när:

9.1.1 Större kampanjer med skadlig kod eller säkerhetsincidenter på endpoints inträffar

9.1.2 Nya hottyper, till exempel fillös skadlig kod eller varianter av ransomware, kräver uppdaterade strategier för detektering eller hantering

9.1.3 Plattformar för endpointskydd eller agentarkitekturer förändras väsentligt

9.1.4 Rättsliga eller regulatoriska krav som påverkar endpointkontroller uppdateras

9.2 Granskningen ska initieras av ansvarig för endpointskydd och samordnas med CISO samt funktionerna för juridik, risk och revision.

9.3 Godkända revideringar ska dokumenteras i registret för dokumentstyrning inom ISMS, tilldelas en ny versionsbeteckning och kommuniceras till alla berörda parter.

9.4 Ersatta versioner ska arkiveras, åtkomstbegränsas och bevaras för att säkerställa revisionsspårets integritet enligt ISMS bevarandetider.

10. Relaterade policyer och kopplingar

10.1 P1 - Informationssäkerhetspolicy. Fastställer grundläggande principer för skydd av system, data och nätverk. Denna policy tillämpar dessa principer på endpointnivå genom tekniska och processrelaterade kontroller mot skadlig kod.

10.2 P4 - Åtkomstkontrollpolicy. Definierar begränsningar för användaråtkomst som tillämpas på endpointnivå, inklusive skydd mot privilegieeskalering och otillåten installation av icke granskad programvara.

10.3 P5 - Ändringshanteringspolicy. Säkerställer att uppdateringar av programvara för endpointskydd, policyregler eller agentkonfigurationer omfattas av godkännande och kontrollerade driftsättningsprocesser.

10.4 P12 - Policy för tillgångshantering. Tillhandahåller den baslinje för tillgångsklassificering och inventering som krävs för synlighet i endpoints, patchtäckning och avgränsning av omfattning för skydd mot skadlig kod.

10.5 P22 - Loggnings- och övervakningspolicy. Möjliggör integration av endpointlarm, agenters hälsostatus och hotinformation i centraliserade SIEM-system för detektering i realtid och forensisk spårbarhet.

10.6 P30 - Incidenthanteringspolicy. Kopplar incidenter med skadlig kod på endpointnivå till standardiserade arbetsflöden för begränsning, eliminering, utredning och återställning med tilldelade roller och eskaleringströsklar.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:

11.1.1 Klausul 8.1 - Operativ planering och styrning: Kräver genomförande av tekniska kontroller, inklusive skyddsåtgärder för endpoints, för att upprätthålla målen för ISMS.

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

11.2.1 Tillhandahåller detaljerad teknisk vägledning om åtgärder mot skadlig kod, säker driftsättning av programvara, övervakning och incidentberedskap för endpointmiljöer.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Skydd mot skadlig kod: Kräver användning av verktyg mot skadlig kod med skanning i realtid, skydd vid åtkomst och beteendeanalys.

11.3.2 SI-4 - Systemövervakning: Stödjer integration av telemetri med centraliserade plattformar för detektering.

11.3.3 CM-6 - Konfigurationsinställningar: Förstärker säker baskonfiguration för endpoints, inklusive tillämpning av skyddsagenter.

11.4 EU:s GDPR (2016/679):

11.4.1 Artikel 32 - Säkerhet i behandlingen: Kräver att organisationer genomför lämpliga tekniska åtgärder för att skydda personuppgifter, inklusive skydd mot hot från skadlig kod.

11.5 EU:s NIS2-direktiv (2022/2555):

11.5.1 Artikel 21(2)(d): Förpliktar verksamheter att införa åtgärder för hotdetektering och förebyggande skydd, inklusive mekanismer för skydd mot skadlig kod på endpointnivå.

11.6 EU:s DORA-förordning (2022/2554):

11.6.1 Artikel 9 - Krav på IKT-riskhantering: Kräver att finansiella entiteter inför skyddsåtgärder för att förebygga, upptäcka och hantera skadlig kod och endpointrelaterade hot.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Skydda mot skadlig kod: Kräver detektering och riskreducering av skadlig kod på alla organisationens endpoints.

11.7.2 DSS01.04 - Hantera tillgänglighet och kapacitet: Säkerställer att skydd mot skadlig kod balanseras mot systemprestanda och verksamhetskontinuitet.

11.7.3 MEA03 - Övervaka, utvärdera och bedöma efterlevnad: Kräver periodisk revision av endpointkontroller och skyddets effektivitet.