					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P20S					Dokumentum címe: **Végpontvédelem – kártevővédelmi szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. fejezet	Operatív kontrollok a kártevők elleni védelemhez
ISO/IEC 27002:2022	8. kontrollcsoport	Kontrollintézkedések a végpontvédelemhez
NIST SP 800-53 Rev.5	SI-3, SI-4	Kártékony kód elleni védelem és incidenskezelés
EU NIS2	21. cikk (2) bekezdés d), e) pont	Kártevővédelem és kockázatkezelés alapvető és fontos szervezetek számára
EU DORA	10. cikk (1) bekezdés, 15. cikk	Működési reziliencia és harmadik felek ellenőrzése
COBIT 2019	DSS05.02, DSS05.04	Végpont- és hálózatvédelem, valamint monitorozás
EU GDPR	32. cikk (1) bekezdés b) pont, 33. cikk	Technikai és szervezeti intézkedések, valamint incidensbejelentés

1. Cél

1.1 Jelen szabályzat meghatározza a laptopok, asztali számítógépek, mobileszközök és hordozható adathordozók kártékony kódokkal szembeni védelmére vonatkozó minimális technikai, eljárási és felhasználói magatartási követelményeket, ideértve a vírusokat, zsarolóvírusokat, kémprogramokat, rootkiteket és egyéb kártevőfenyegetéseket.

1.2 A szabályzat célja annak biztosítása, hogy a végpontok kialakítása, karbantartása és használata csökkentse a kártevőfertőzés, a továbbterjedés és a rendszerek kompromittálódásának kockázatát.

1.3 A szervezet elismeri, hogy a végpontok a kártevők gyakori belépési pontjai, ezért azokat előírt alapbeállításokkal kell megerősíteni, felügyelni, valamint többrétegű védelemmel kell ellátni.

1.4 A szabályzat támogatja a szervezet ISO/IEC 27001:2022 tanúsítási célkitűzéseit, és összhangban áll a GDPR-ral, a NIS2 irányelvvel, a DORA rendelettel és más releváns keretrendszerekkel.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 Valamennyi szervezeti végpontra, beleértve az asztali számítógépeket, laptopokat, táblagépeket, mobiltelefonokat és értékesítési ponti terminálokat

2.1.2 Az üzleti alkalmazásokhoz vagy adatokhoz való hozzáférésre használt BYOD (saját tulajdonú) eszközökre

2.1.3 Az eltávolítható tárolóeszközökre, például USB-meghajtókra és külső merevlemezekre

2.1.4 Az ezeken a platformokon futó valamennyi operációs rendszerre, végponti szoftverre és kommunikációs eszközre

2.2 A szabályzat egyaránt vonatkozik:

2.2.1 A belső munkatársakra, vállalkozókra, gyakornokokra és menedzselt szolgáltatókra (MSP-kre)

2.2.2 A helyszínen, távolról vagy hibrid munkavégzés keretében használt eszközökre

2.2.3 Az üzleti vagy személyes adatokat tároló, felhőkapcsolattal rendelkező vagy offline végpontokra

3. Célkitűzések

3.1 A kártevőfertőzések és azok továbbterjedésének megelőzése a belső rendszerekben, a felhasználói eszközökön és a külső kapcsolatokon keresztül

3.2 A kártevőkhöz kapcsolódó fenyegetések gyors észlelése és elszigetelése automatizált végpontbiztonsági technológiák és meghatározott eszkalációs útvonalak alkalmazásával

3.3 Annak biztosítása, hogy üzleti információkhoz kizárólag engedélyezett, védett és felügyelt eszközökkel lehessen hozzáférni

3.4 Egyértelmű munkatársi felelősségi körök és felhasználói magatartási szabályok érvényesítése a kártevőkhöz kapcsolódó incidensek kockázatának csökkentése érdekében

3.5 A kártevőészlelésekkel, a reagálási lépésekkel és a szabályzatnak való megfeleléssel kapcsolatos, visszakövethető és auditálható nyilvántartások fenntartása

3.6 A személyes és üzleti adatok védelme a kártevők miatti kompromittálódással szemben többrétegű védelmi stratégiák alkalmazásával

4. Szerepkörök és felelősségi körök

4.1 Ügyvezető

4.1.1 A szabályzat tulajdonosa, és biztosítja, hogy a végpontvédelemhez elegendő erőforrás álljon rendelkezésre

4.1.2 Jóváhagyja a vírusvédelmi szoftvereket, a mobileszköz-kezelési (MDM) megoldásokat és a harmadik felek hozzáférésére vonatkozó szabályokat

4.1.3 Felülvizsgálja a végpontokat érintő kártevőincidensek jelentéseit, a hatásösszefoglalókat és az incidensbejelentéseket

4.2 IT-támogatás / belső informatikai rendszergazda

4.2.1 Kiválasztja és bevezeti a vírusvédelmi, kártevővédelmi, valamint a végponti észlelési és reagálási (EDR) megoldásokat

4.2.2 Biztosítja az egységes frissítést és a naplók megőrzését

4.2.3 Reagál a kártevőriasztásokra, elkülöníti a fertőzött rendszereket, és végrehajtja a helyesbítő intézkedéseket

4.2.4 Érvényesíti az USB-eszközök és egyéb külső eszközök használatára vonatkozó kontrollokat

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1 Éves felülvizsgálati követelmény

9.1.1 Jelen szabályzatot évente legalább egyszer formálisan felül kell vizsgálni az ügyvezető által, az IT-támogatással és az adatvédelmi koordinátorral együttműködésben

9.2 Kiváltó eseményhez kötött frissítések

9.2.1 A szabályzatot akkor is frissíteni kell, ha:

9.2.1.1 Új, jelentős kártevőfenyegetés vagy kártevőkitörés a szervezet által használt végpontokat célozza

9.2.1.2 A vírusvédelmi vagy EDR-eszközöket módosítják, fejlesztik vagy lecserélik

9.2.1.3 Egy kártevőincidens feltárja a szabályzat hatályával vagy alkalmazásával kapcsolatos hiányosságokat

9.2.1.4 A jogi vagy szabályozási követelmények (pl. GDPR, DORA, NIS2) változnak

9.3 Verziókezelés és kommunikáció

9.3.1 Valamennyi szabályzatmódosítást dokumentálni kell verziószámmal, dátummal és a változások összefoglalásával

9.3.2 A munkatársakat értesíteni kell a frissítésekről, különösen akkor, ha azok az operatív vagy felhasználói magatartási követelményeket érintik

9.3.3 A korábbi verziókat legalább 3 évig meg kell őrizni a szabályzatarchívumban az auditok támogatása érdekében

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi KKV-szabályzatokkal együtt kell alkalmazni:

10.1.1 P9S – Távmunka-szabályzat: biztosítja, hogy a végpontvédelmi követelmények a telephelyen kívül vagy hibrid munkavégzési környezetben használt eszközökre is érvényesüljenek

10.1.2 P12S – Eszközkezelési szabályzat: támogatja valamennyi végpont nyomon követését és szabályozását, biztosítva, hogy kizárólag engedélyezett és védett eszközök legyenek használatban

10.1.3 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: megerősíti, hogy a kártevők megelőzése alapvető adatvédelmi kontroll a személyes és érzékeny adatok kompromittálódásának megelőzésére

10.1.4 P22S – Naplózási és felügyeleti szabályzat: meghatározza a kártevőesemények naplózására és a korai reagálást támogató riasztási láthatóság fenntartására vonatkozó követelményeket

10.1.5 P30S – Incidenskezelési szabályzat: meghatározza az eszkaláció, az elszigetelés és a külső értesítés lépéseit, ha a kártevő adatkompromittálódáshoz vagy működési zavarhoz vezet

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001

11.1.1 8.1 pont – Előírja az olyan kockázatok csökkentését szolgáló operatív kontrollok bevezetését, mint a kártevőtámadások

11.2 ISO/IEC 27002

11.2.1 8.7 kontroll – Részletezi a kártevővédelmi gyakorlatokat, beleértve a vírusvédelmet, a valós idejű vizsgálatot, a frissítéseket és a felhasználói képzést

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Előírja a kártékony kód elleni védelmi mechanizmusok bevezetését a végpontokon

11.3.2 SI-4 – Kötelezővé teszi a végpontszintű fenyegetések és riasztások monitorozását, észlelését, elemzését és a reagálási intézkedéseket

11.4 EU GDPR

11.4.1 32. cikk (1) bekezdés b) pont – Előírja a személyes adatok védelméhez szükséges technikai és szervezeti kontrollokat, például a vírusvédelmet

11.4.2 33. cikk – Kötelezővé teszi az incidensbejelentést, ha a kártevő az adatok sértetlenségét, bizalmasságát vagy rendelkezésre állását veszélyezteti

11.5 EU NIS2 irányelv

11.5.1 21. cikk (2) bekezdés d) pont – Előírja a kártevőfenyegetések megelőzését és kezelését szolgáló intézkedéseket az alapvető és fontos szervezeteknél

11.5.2 21. cikk (2) bekezdés e) pont – Kötelezővé teszi a rétegzett kiberbiztonsági kockázatkezelési stratégiákat, beleértve a végponti kártevővédelmet

11.6 EU DORA

11.6.1 10. cikk (1) bekezdés – Előírja, hogy az IKT-rendszereket a működési reziliencia részeként védeni kell a kártevőkkel és más fenyegetésekkel szemben

11.6.2 15. cikk – Kötelezővé teszi a pénzügyi szervezetek számára a kártevővédelem ellenőrzését a harmadik fél szolgáltatóknál

11.7 COBIT 2019

11.7.1 DSS05.02 – Hangsúlyozza a végpontok és hálózatok kártevőfenyegetésekkel szembeni védelmét szolgáló intézkedéseket

11.7.2 DSS05.04 – Támogatja a kártevőkhöz kapcsolódó biztonsági események monitorozását és riasztását a folyamatos működés részeként