					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P20S					Dokumento pavadinimas: **Galinių įrenginių apsaugos nuo kenkėjiškos programinės įrangos politika**						
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:						
X	Politika		Standartas		Procedūra		Forma		Registras		Kita

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	Operacinės kontrolės priemonės apsaugai nuo kenkėjiškos programinės įrangos
ISO/IEC 27002:2022	8 kontrolės priemonė	Kontrolės priemonės galinių įrenginių apsaugai
NIST SP 800-53 Rev.5	SI-3, SI-4	Apsauga nuo kenkėjiško kodo ir reagavimas į incidentus
ES NIS2 direktyva	21 straipsnio 2 dalies d ir e punktai	Apsauga nuo kenkėjiškos programinės įrangos ir rizikos valdymas esminiams ir svarbiems subjektams
ES DORA reglamentas	10 straipsnio 1 dalis, 15 straipsnis	Operacinis atsparumas ir trečiųjų šalių tikrinimas
COBIT 2019	DSS05.02, DSS05.04	Galinių įrenginių ir tinklo apsauga bei stebėsena
ES BDAR	32 straipsnio 1 dalies b punktas, 33 straipsnis	Techninės ir organizacinės priemonės bei pranešimas apie pažeidimą

1. Tikslas

1.1 Ši politika nustato minimalius techninius, procedūrinius ir elgsenos reikalavimus, skirtus apsaugoti visus galinius įrenginius, įskaitant nešiojamuosius ir stacionariuosius kompiuterius, mobiliuosius įrenginius ir nešiojamąsias laikmenas, nuo kenkėjiško kodo, įskaitant virusus, išpirkos reikalaujančią programinę įrangą, šnipinėjimo programinę įrangą, rootkit tipo kenkimo programinę įrangą ir kitas kenkėjiškos programinės įrangos grėsmes.

1.2 Šios politikos tikslas – užtikrinti, kad galiniai įrenginiai būtų aprūpinti apsaugos priemonėmis, prižiūrimi ir naudojami taip, kad būtų mažinama kenkėjiškos programinės įrangos infekcijos, plitimo ir sistemų kompromitavimo rizika.

1.3 Organizacija pripažįsta, kad galiniai įrenginiai yra dažni kenkėjiškos programinės įrangos patekimo taškai, todėl jie privalo būti stiprinami, stebimi ir apsaugoti taikant daugiasluoksnę gynybą.

1.4 Ši politika padeda siekti organizacijos ISO/IEC 27001:2022 sertifikavimo tikslų ir yra suderinta su ES Bendruoju duomenų apsaugos reglamentu (BDAR), NIS2 direktyva, Skaitmeninio operacinio atsparumo aktu (DORA) ir kitomis aktualiomis sistemomis.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems organizacijos galiniams įrenginiams, įskaitant stacionariuosius kompiuterius, nešiojamuosius kompiuterius, planšetinius kompiuterius, mobiliuosius telefonus ir pardavimo vietų terminalus

2.1.2 Asmeniniams įrenginiams, naudojamiems prieigai prie verslo taikomųjų programų ar duomenų pagal nuosavų įrenginių naudojimo (BYOD) modelį

2.1.3 Išimamiems duomenų saugojimo įrenginiams, pavyzdžiui, USB laikmenoms ir išoriniams standiesiems diskams

2.1.4 Bet kokioms operacinėms sistemoms, galinių įrenginių programinei įrangai ar komunikacijos priemonėms, veikiančioms šiose platformose

2.2 Ji vienodai taikoma:

2.2.1 Vidaus darbuotojams, rangovams, praktikantams ir valdomų paslaugų teikėjams (MSP)

2.2.2 Įrenginiams, naudojamiems vietoje, nuotoliniu būdu arba pagal hibridinio darbo modelį

2.2.3 Prie debesijos prijungtiems ar neprisijungusiems galiniams įrenginiams, kuriuose saugomi veiklos ar asmens duomenys

3. Tikslai

3.1 Užkirsti kelią kenkėjiškos programinės įrangos infekcijai ir plitimui vidaus sistemose, naudotojų įrenginiuose ir išoriniuose ryšiuose

3.2 Greitai aptikti ir lokalizuoti su kenkėjiška programine įranga susijusias grėsmes naudojant automatizuotas galinių įrenginių saugos technologijas ir apibrėžtus eskalavimo kelius

3.3 Užtikrinti, kad prieigai prie veiklos informacijos būtų naudojami tik autorizuoti, apsaugoti ir stebimi įrenginiai

3.4 Nustatyti aiškias darbuotojų atsakomybes ir naudotojų elgsenos taisykles, kad būtų mažinama su kenkėjiška programine įranga susijusių incidentų rizika

3.5 Tvarkyti atsekamus ir audituojamus įrašus apie kenkėjiškos programinės įrangos aptikimą, reagavimą ir politikos laikymąsi

3.6 Apsaugoti asmens ir veiklos duomenis nuo kompromitavimo dėl kenkėjiškos programinės įrangos taikant daugiasluoksnės gynybos strategijas

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 Yra šios politikos savininkas ir užtikrina, kad galinių įrenginių apsaugai būtų skiriami pakankami ištekliai

4.1.2 Tvirtina antivirusinės programinės įrangos, mobiliųjų įrenginių valdymo (MDM) priemonių ir trečiųjų šalių prieigos taisykles

4.1.3 Peržiūri pranešimus apie kenkėjiškos programinės įrangos incidentus, poveikio santraukas ir pranešimus apie pažeidimus, susijusius su galiniais įrenginiais

4.2 IT paslaugų teikėjas / vidaus IT administratorius

4.2.1 Parenka ir diegia antivirusinę programinę įrangą, apsaugos nuo kenkėjiškos programinės įrangos priemones ir galinių įrenginių aptikimo ir reagavimo (EDR) sprendimus

4.2.2 Užtikrina, kad atnaujinimai būtų diegiami nuosekliai, o žurnalai būtų saugomi

4.2.3 Reaguoja į įspėjimus apie kenkėjišką programinę įrangą, izoliuoja užkrėstas sistemas ir vykdo taisomuosius veiksmus

4.2.4 Taiko USB ir išorinių įrenginių naudojimo kontrolės priemones

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Kasmetinės peržiūros reikalavimas

9.1.1 Ši politika privalo būti formaliai peržiūrima ne rečiau kaip kartą per metus generalinio vadovo, koordinuojant su IT paslaugų teikėju ir privatumo koordinatoriumi

9.2 Atnaujinimai pagal suveikimo įvykius

9.2.1 Politika taip pat privalo būti atnaujinta, kai:

9.2.1.1 Nauja reikšminga kenkėjiškos programinės įrangos grėsmė ar protrūkis nukreiptas į organizacijos naudojamus galinius įrenginius

9.2.1.2 Antivirusinės programinės įrangos ar EDR priemonės pakeičiamos, atnaujinamos arba pakeičiamos naujomis

9.2.1.3 Kenkėjiškos programinės įrangos incidentas atskleidžia šios politikos taikymo srities ar įgyvendinimo silpnąsias vietas

9.2.1.4 Atnaujinami teisiniai ar reglamentavimo reikalavimai (pvz., BDAR, DORA, NIS2)

9.3 Versijų kontrolė ir komunikacija

9.3.1 Visi politikos pakeitimai privalo būti dokumentuojami nurodant versijos numerį, datą ir pakeitimų santrauką

9.3.2 Darbuotojai privalo būti informuojami apie atnaujinimus, ypač jei jie keičia operacinius ar elgsenos reikalavimus

9.3.3 Ankstesnės politikos versijos archyve privalo būti saugomos ne trumpiau kaip 3 metus auditams pagrįsti

10. Susijusios politikos ir sąsajos

10.1 Ši politika privalo būti įgyvendinama kartu su šiomis MVĮ politikomis:

10.1.1 P9S – Nuotolinio darbo politika: užtikrina, kad galinių įrenginių apsaugos reikalavimai būtų taikomi įrenginiams, naudojamiems ne organizacijos vietoje arba hibridinio darbo sąlygomis

10.1.2 P12S – Turto valdymo politika: padeda užtikrinti visų galinių įrenginių apskaitą ir kontrolę, kad būtų naudojami tik autorizuoti ir apsaugoti įrenginiai

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: sustiprina kenkėjiškos programinės įrangos prevenciją kaip pagrindinę privatumo kontrolės priemonę, skirtą apsaugoti asmens ir jautrius duomenis nuo kompromitavimo

10.1.4 P22S – Žurnalų tvarkymo ir stebėsenos politika: nustato reikalavimus kenkėjiškos programinės įrangos įvykių registravimui ir įspėjimų matomumo užtikrinimui ankstyvam reagavimui

10.1.5 P30S – Reagavimo į incidentus politika: apibrėžia eskalavimo, lokalizavimo ir išorinio pranešimo veiksmus, jei kenkėjiška programinė įranga sukelia duomenų kompromitavimą arba operacinį sutrikimą

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas – reikalauja įgyvendinti operacines kontrolės priemones, skirtas mažinti tokias rizikas kaip kenkėjiškos programinės įrangos atakos

11.2 ISO/IEC 27002

11.2.1 8.7 kontrolės priemonė – apibrėžia apsaugos nuo kenkėjiškos programinės įrangos praktikas, įskaitant antivirusinę programinę įrangą, skenavimą realiuoju laiku, atnaujinimus ir naudotojų mokymą

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – reikalauja galiniuose įrenginiuose diegti apsaugos nuo kenkėjiško kodo mechanizmus

11.3.2 SI-4 – nustato stebėsenos, aptikimo, analizės ir reagavimo veiksmų reikalavimus galinių įrenginių lygmens grėsmėms ir įspėjimams

11.4 ES BDAR

11.4.1 32 straipsnio 1 dalies b punktas – reikalauja techninių ir organizacinių kontrolės priemonių (pavyzdžiui, antivirusinės programinės įrangos) asmens duomenims apsaugoti

11.4.2 33 straipsnis – įpareigoja pranešti apie pažeidimą, kai kenkėjiška programinė įranga pažeidžia duomenų vientisumą, konfidencialumą ar prieinamumą

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies d punktas – reikalauja taikyti priemones, skirtas užkirsti kelią kenkėjiškos programinės įrangos grėsmėms ir į jas reaguoti esminiuose ir svarbiuose subjektuose

11.5.2 21 straipsnio 2 dalies e punktas – nustato daugiasluoksnių kibernetinio saugumo rizikos valdymo strategijų, įskaitant galinių įrenginių apsaugą nuo kenkėjiškos programinės įrangos, reikalavimą

11.6 ES DORA reglamentas

11.6.1 10 straipsnio 1 dalis – reikalauja, kad IRT sistemos būtų apsaugotos nuo kenkėjiškos programinės įrangos ir kitų grėsmių kaip operacinio atsparumo dalis

11.6.2 15 straipsnis – įpareigoja finansų organizacijas tikrinti apsaugą nuo kenkėjiškos programinės įrangos trečiųjų šalių paslaugų teikėjų aplinkose

11.7 COBIT 2019

11.7.1 DSS05.02 – pabrėžia apsaugos priemones, skirtas apsaugoti galinius įrenginius ir tinklus nuo kenkėjiškos programinės įrangos grėsmių

11.7.2 DSS05.04 – palaiko stebėseną ir įspėjimus apie su kenkėjiška programine įranga susijusius saugumo įvykius kaip nuolatinių operacijų dalį