| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Čia įrašykite registruoto juridinio asmens pavadinimą | | | | | | |
| Dokumento numeris:<br>P20 | | | | | Dokumento pavadinimas:<br>**Galinių įrenginių apsaugos / apsaugos nuo kenkėjiškos programinės įrangos politika** | | | | | | |
| Versija:<br>1.0 | | Įsigaliojimo data:<br>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 | Galinių įrenginių apsaugos ir apsaugos nuo kenkėjiškos programinės įrangos kontrolės priemonės yra privalomos ISVS tikslams pasiekti |
| ISO/IEC 27002:2022 | Kontrolės priemonės 8.7, 8 | Pateikia technines kontrolės priemones ir gaires dėl apsaugos nuo kenkėjiškos programinės įrangos, galinių įrenginių apsaugos ir incidentų valdymo |
| NIST SP 800-53 Rev.5 | SI-3, SI-4, CM-6 | Apibrėžia apsaugos nuo kenkėjiško kodo, centralizuotos stebėsenos ir bazinės konfigūracijos reikalavimus |
| ES BDAR | 32 straipsnis | Nustato pareigą taikyti tinkamas technines priemones asmens duomenims apsaugoti, įskaitant apsaugą nuo kenkėjiškos programinės įrangos |
| ES NIS2 direktyva | 21 straipsnio 2 dalies d punktas | Reikalauja diegti galinių įrenginių lygmens grėsmių aptikimo ir prevencijos priemones |
| ES DORA reglamentas | 9 straipsnis | Reikalauja IRT rizikos valdymo priemonių, skirtų apsaugai nuo kenkėjiškos programinės įrangos ir per galinius įrenginius plintančių grėsmių |
| COBIT 2019 | DSS05.01, DSS01.04, MEA | Nustato galinių įrenginių kontrolės priemonių apsaugos, stebėsenos ir vertinimo reikalavimus |

**1. Tikslas**

1.1 Ši politika nustato privalomas kontrolės priemones ir veiklos reikalavimus, skirtus organizacijos galinių įrenginių, įskaitant stalinius kompiuterius, nešiojamuosius kompiuterius, mobiliuosius įrenginius ir serverius, apsaugai nuo kenkėjiškos programinės įrangos ir susijusių grėsmių.

1.2 Ji nustato minimalius galinių įrenginių apsaugos, kenkėjiškos programinės įrangos aptikimo, lokalizavimo, reagavimo ir elgsenos stebėsenos standartus, užtikrinančius, kad sistemos išliktų atsparios tiek plačiai paplitusioms, tiek pažangioms kenkėjiškos programinės įrangos atmainoms.

1.3 Ši politika tiesiogiai palaiko atitiktį ISO/IEC 27001:2022 8.1 skyriui ir A priedo kontrolei 8.7 bei yra suderinta su regioniniais kibernetinio saugumo įpareigojimais pagal ES BDAR, NIS2 direktyvą ir DORA reglamentą.

**2. Taikymo sritis**

**2.1 Ši politika taikoma visiems galiniams įrenginiams, įskaitant:**

2.1.1 organizacijai priklausančius arba organizacijos valdomus stalinius kompiuterius, nešiojamuosius kompiuterius, mobiliuosius įrenginius ir virtualių egzempliorių aplinkas;

2.1.2 asmeninius įrenginius, leidžiamus pagal nuosavų įrenginių naudojimo politiką, kai taikomas MDM arba įdiegiami galinių įrenginių agentai;

2.1.3 serverius ir infrastruktūros turtą, įskaitant debesijoje veikiančias virtualiąsias mašinas ir kraštinius įrenginius;

2.1.4 operacines sistemas, tvarkykles, vietines paslaugas, galinių įrenginių agentus ir saugumo kontrolės priemones, įdiegtas kiekviename mazge.

**2.2 Ši politika taikoma visam personalui, turinčiam administracinę, techninę arba operacinę atsakomybę už bet kurį galinį įrenginį, įskaitant:**

2.2.1 vidaus darbuotojus ir rangovus;

2.2.2 valdomųjų paslaugų teikėjus (MSP), išorines darbo vietų palaikymo paslaugas ir trečiųjų šalių IT administratorius;

2.2.3 naudotojus, kuriems leidžiama naudoti nešiojamąsias sistemas, nešiojamuosius kompiuterius su virtualiuoju privačiuoju tinklu (VPN) arba mobiliaja prieiga prie organizacijos tinklų.

**2.3 Šios politikos taikomos grėsmės apima, bet tuo neapsiriboja:**

2.3.1 virusus, kirminus, Trojos arklius, išpirkos reikalaujančią programinę įrangą, šnipinėjimo programinę įrangą, rootkit tipo kenkėjišką programinę įrangą, reklamines programas, klavišų paspaudimų registratorius ir botnetus;

2.3.2 failų nenaudojančią kenkėjišką programinę įrangą, nulinės dienos pažeidžiamumų išnaudojimo priemones, privilegijų pakėlimo kenkėjišką programinę įrangą ir naršyklės išnaudojimo rinkinius;

2.3.3 kenkėjišką kodą, platinamą per išimamas laikmenas, fišingo vektorius, automatinius atsisiuntimus lankantis svetainėse arba USB pagrindu vykdomas atakas.

## 3. Tikslai

3.1 Apsaugoti galinių įrenginių sistemų vientisumą, prieinamumą ir konfidencialumą bei jų tvarkomus duomenis taikant patikimą prevenciją, aptikimą ir reagavimą į kenkėjišką programinę įrangą.

3.2 Užkirsti kelią kenkėjiško kodo vykdymui ar plitimui organizacijos tinkluose taikant technines apsaugos priemones, bazinį stiprinimą ir realiojo laiko telemetriją.

3.3 Integruoti galinių įrenginių apsaugą su kitomis ISVS kontrolės priemonėmis, įskaitant pažeidžiamumų valdymą, prieigos kontrolę, žurnalų tvarkymą ir stebėseną bei reagavimą į incidentus.

3.4 Užtikrinti nuolatinį galinių įrenginių matomumą per centralizuotai valdomas apsaugos platformas, įskaitant antivirusinę / apsaugos nuo kenkėjiškos programinės įrangos programinę įrangą, galinių įrenginių aptikimą ir reagavimą (EDR) ir SIEM telemetriją.

3.5 Užtikrinti teisinių, reglamentavimo ir standartų reikalavimų, nustatančių galinių įrenginių saugumą, laikymąsi, pvz., ES BDAR 32 straipsnio, NIS2 direktyvos 21 straipsnio ir DORA reglamento 9 straipsnio.

3.6 Apibrėžti atskaitingus vaidmenis, nustatyti pataisų diegimo ir reagavimo į įspėjimus SLA bei užtikrinti pasirengimą auditui per dokumentaciją ir ataskaitų teikimą.

## 4. Vaidmenys ir atsakomybė

**4.1 informacijos saugumo vadovas (CISO)**

4.1.1 yra šios politikos savininkas ir užtikrina jos suderinamumą su ISVS ir bendra saugumo strategija;

4.1.2 kas ketvirtį peržiūri galinių įrenginių apsaugos rodiklius, incidentų tendencijas ir priemonių veiksmingumą;

4.1.3 tvirtina išimtis ir likutinės rizikos prisiėmimą, susijusį su galinių įrenginių aprėptimi.

**4.2 Galinių įrenginių saugumo vadovas / saugumo operacijų centro vadovas**

4.2.1 valdo galinių įrenginių apsaugos sistemas, pvz., AV, EDR ir MDM;

4.2.2 vykdo politikos taikymo priežiūrą, grėsmių aptikimo derinimą ir reagavimo veiksmų planų valdymą;

4.2.3 palaiko aprėpties statistiką, kenkėjiškos programinės įrangos incidentų žurnalus ir įspėjimų konfigūracijos bazinius rinkinius.

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

**9. Peržiūros ir atnaujinimo reikalavimai**

**9.1 Ši politika turi būti peržiūrima kasmet arba kai:**

9.1.1 įvyksta didelės apimties kenkėjiškos programinės įrangos kampanijos arba galinių įrenginių saugumo incidentai;

9.1.2 nauji grėsmių tipai, pvz., failų nenaudojanti kenkėjiška programinė įranga ar išpirkos reikalaujančios programinės įrangos variantai, reikalauja atnaujintų aptikimo ar reagavimo strategijų;

9.1.3 reikšmingai pasikeičia galinių įrenginių apsaugos platformos arba agentų architektūros;

9.1.4 atnaujinami teisiniai ar reglamentavimo reikalavimai, turintys įtakos galinių įrenginių kontrolės priemonėms.

9.2 Peržiūrą turi inicijuoti galinių įrenginių saugumo vadovas, koordinuodamas veiksmus su CISO, teisine, rizikos valdymo ir audito funkcijomis.

9.3 Patvirtinti pakeitimai turi būti dokumentuojami ISVS dokumentų kontrolės registre, jiems turi būti suteikiamas naujas versijos identifikatorius, o apie juos turi būti informuotos visos susijusios šalys.

9.4 Pakeistos versijos turi būti archyvuojamos, jų prieiga ribojama ir jos saugomos pagal ISVS saugojimo grafikus, siekiant užtikrinti audito pėdsako vientisumą.

**10. Susijusios politikos ir sąsajos**

10.1 P1 – Informacijos saugumo politika. Nustato pagrindinius sistemų, duomenų ir tinklų apsaugos principus. Ši politika įgyvendina tuos principus galinių įrenginių lygmeniu taikant technines ir procedūrines apsaugos nuo kenkėjiškos programinės įrangos kontrolės priemones.

10.2 P4 – Prieigos kontrolės politika. Apibrėžia naudotojų prieigos apribojimus, kurie taikomi galinių įrenginių lygmeniu, įskaitant apsaugą nuo privilegijų pakėlimo ir neperžiūrėtos programinės įrangos diegimo.

10.3 P5 – Pakeitimų valdymo politika. Užtikrina, kad galinių įrenginių apsaugos programinės įrangos, politikos taisyklių ar agentų konfigūracijų atnaujinimams būtų taikomi tvirtinimo ir kontroliuojamo diegimo procesai.

10.4 P12 – Turto valdymo politika. Nustato turto klasifikavimo ir apskaitos bazę, reikalingą galinių įrenginių matomumui, pataisų aprėpčiai ir apsaugos nuo kenkėjiškos programinės įrangos taikymo sričiai apibrėžti.

10.5 P22 – Žurnalų tvarkymo ir stebėsenos politika. Sudaro sąlygas integruoti galinių įrenginių įspėjimus, agentų būseną ir grėsmių žvalgybą į centralizuotas SIEM sistemas realiojo laiko aptikimui ir skaitmeninės kriminalistikos atsekamumui.

10.6 P30 – Reagavimo į incidentus politika. Susieja galinių įrenginių lygmeniu nustatytus kenkėjiškos programinės įrangos incidentus su standartizuotomis lokalizavimo, pašalinimo, tyrimo ir atkūrimo darbo eigomis bei priskirtais vaidmenimis ir eskalavimo slenksčiais.

**11. Pamatiniai standartai ir sistemos**

**11.1 ISO/IEC 27001:**

11.1.1 8.1 skyrius – Veiklos planavimas ir kontrolė: reikalauja įgyvendinti technines kontrolės priemones, įskaitant galinių įrenginių apsaugos priemones, siekiant išlaikyti ISVS tikslus.

**11.2 ISO/IEC 27002:2022 – Kontrolės priemonės 8.7, 8:**

11.2.1 pateikia išsamias technines gaires dėl apsaugos nuo kenkėjiškos programinės įrangos priemonių, saugaus programinės įrangos diegimo, stebėsenos ir pasirengimo incidentams galinių įrenginių aplinkose.

**11.3 NIST SP 800-53 Rev.5:**

11.3.1 SI-3 – Apsauga nuo kenkėjiško kodo: reikalauja naudoti apsaugos nuo kenkėjiškos programinės įrangos priemones su realiojo laiko skenavimu, apsauga prieigos metu ir elgsenos analize.

11.3.2 SI-4 – Sistemų stebėsena: palaiko telemetrijos integraciją su centralizuotomis aptikimo platformomis.

11.3.3 CM-6 – Konfigūracijos nustatymai: sustiprina bazinius galinių įrenginių kontrolės nustatymus, įskaitant apsaugos agentų taikymą.

**11.4 ES BDAR (2016/679):**

11.4.1 32 straipsnis – Tvarkymo saugumas: reikalauja, kad organizacijos įgyvendintų tinkamas technines priemones asmens duomenims apsaugoti, įskaitant apsaugą nuo kenkėjiškos programinės įrangos grėsmių.

**11.5 ES NIS2 direktyva (2022/2555):**

11.5.1 21 straipsnio 2 dalies d punktas: įpareigoja subjektus diegti grėsmių aptikimo ir prevencijos priemones, įskaitant apsaugos nuo kenkėjiškos programinės įrangos mechanizmus galinių įrenginių lygmeniu.

**11.6 ES DORA reglamentas (2022/2554):**

11.6.1 9 straipsnis – IRT rizikos valdymo reikalavimai: nustato, kad finansų subjektai turi taikyti apsaugos priemones, skirtas užkirsti kelią kenkėjiškai programinei įrangai ir per galinius įrenginius plintančioms grėsmėms, jas aptikti ir į jas reaguoti.

**11.7 COBIT 2019:**

11.7.1 DSS05.01 – Apsauga nuo kenkėjiškos programinės įrangos: nustato kenkėjiškos programinės įrangos aptikimo ir mažinimo reikalavimus visuose organizacijos galiniuose įrenginiuose.

11.7.2 DSS01.04 – Prieinamumo ir pajėgumų valdymas: užtikrina, kad apsauga nuo kenkėjiškos programinės įrangos būtų suderinta su sistemos našumu ir veiklos tęstinumu.

11.7.3 MEA03 – Atitikties stebėsena, vertinimas ir peržiūra: reikalauja periodinio galinių įrenginių kontrolės priemonių ir apsaugos veiksmingumo audito.