					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P20					Dokumenta nosaukums: **Galiekārtu aizsardzības/ļaunatūras politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Galiekārtu aizsardzība un aizsardzības līdzekļi pret ļaunprogrammatūru ir nepieciešami, lai sasniegtu IDPS mērķus
ISO/IEC 27002:2022	Kontroles pasākumi 8.7, 8	Nosaka tehniskos kontroles pasākumus un vadlīnijas aizsardzībai pret ļaunprogrammatūru, galiekārtu aizsardzībai un incidentu pārvaldībai
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Nosaka prasības aizsardzībai pret ļaunprātīgu kodu, centralizētai uzraudzībai un pamatkonfigurācijai
ES GDPR	32. pants	Nosaka pienākumu ieviest atbilstošus tehniskos pasākumus personas datu aizsardzībai, tostarp aizsardzību pret ļaunatūru
ES NIS2	21. panta 2. punkta d) apakšpunkts	Prasa ieviest galiekārtu līmeņa apdraudējumu noteikšanas un preventīvos pasākumus
ES DORA	9. pants	Prasa IKT risku pārvaldību aizsardzībai pret ļaunatūru un no galiekārtām izrietošiem apdraudējumiem
COBIT 2019	DSS05.01, DSS01.04, MEA	Nosaka prasības galiekārtu kontroles pasākumu aizsardzībai, uzraudzībai un izvērtēšanai

1. Mērķis

1.1 Šī politika nosaka obligātos kontroles pasākumus un darbības prasības organizācijas galiekārtu, tostarp galddatoru, klēpjdatoru, mobilo ierīču un serveru, aizsardzībai pret ļaunatūru un saistītajiem apdraudējumiem.

1.2 Tā nosaka minimālos standartus galiekārtu aizsardzībai, ļaunatūras noteikšanai, ierobežošanai, reaģēšanai un uzvedības uzraudzībai, nodrošinot sistēmu noturību gan pret plaši izplatītiem, gan sarežģītiem ļaunatūras paveidiem.

1.3 Šī politika tieši atbalsta atbilstību ISO/IEC 27001:2022 8. punktam un A pielikuma 8.7. kontrolei, kā arī ir saskaņota ar reģionālajiem kiberdrošības pienākumiem saskaņā ar GDPR, NIS2 un DORA.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām galiekārtām, tostarp:

2.1.1 organizācijai piederošiem vai organizācijas pārvaldītiem galddatoriem, klēpjdatoriem, mobilajām ierīcēm un virtuālajām instancēm;

2.1.2 personīgajām ierīcēm, kas autorizētas saskaņā ar privāto ierīču izmantošanas politiku un kurām piemērota MDM vai galiekārtas aģenta uzstādīšana;

2.1.3 serveriem un infrastruktūras aktīviem, tostarp mākoņvidē izvietotām virtuālajām mašīnām un tīkla malas ierīcēm;

2.1.4 operētājsistēmām, draiveriem, lokālajiem pakalpojumiem, galiekārtu aģentiem un drošības kontroles pasākumiem, kas uzstādīti katrā mezglā.

2.2 Šī politika attiecas uz visu personālu, kam ir administratīva, tehniska vai operatīva atbildība par jebkuru galiekārtu, tostarp:

2.2.1 iekšējiem darbiniekiem un līgumslēdzējiem;

2.2.2 pārvaldīto pakalpojumu sniedzējiem (MSP), ārpakalpojumu darbvietu atbalsta sniedzējiem un trešo pušu IT administratoriem;

2.2.3 lietotājiem, kuri ir autorizēti izmantot pārnēsājamas sistēmas, ar VPN aprīkotus klēpjdatorus vai mobilo piekļuvi organizācijas tīkliem.

2.3 Šīs politikas aptvertie apdraudējumi ietver, bet neaprobežojas ar:

2.3.1 vīrusiem, tārpiem, Trojas zirgiem, izspiedējprogrammatūru, spiegprogrammatūru, rootkit tipa ļaunatūru, reklāmprogrammatūru, taustiņspiedienu pārtveršanas programmatūru un robottīkliem;

2.3.2 bezfailu ļaunatūru, nulltās dienas izpildslodzēm, privilēģiju paaugstināšanas ļaunatūru un pārlūkprogrammu ekspluatācijas rīkkopām;

2.3.3 ļaunprātīgu kodu, kas tiek piegādāts ar noņemamiem datu nesējiem, pikšķerēšanas vektoriem, automātiskām lejupielādēm vai USB balstītiem uzbrukumiem.

3. Mērķi

3.1 Aizsargāt galiekārtu sistēmu integritāti, pieejamību un konfidencialitāti, kā arī tajās apstrādātos datus, izmantojot efektīvu ļaunatūras novēršanu, noteikšanu un reaģēšanu.

3.2 Novērst ļaunprātīga koda izpildi vai izplatīšanos organizācijas tīklos, piemērojot tehniskos drošības pasākumus, pamatkonfigurāciju un reāllaika telemetriju.

3.3 Integrēt galiekārtu aizsardzību ar citiem IDPS kontroles pasākumiem, tostarp ievainojamību pārvaldību, piekļuves kontroli, žurnālfiksēšanu un uzraudzību, kā arī incidentu apstrādi.

3.4 Nodrošināt nepārtrauktu galiekārtu pārskatāmību, izmantojot centralizēti pārvaldītas aizsardzības platformas, tostarp antivīrusu/pretļaunatūras risinājumus, galiekārtu noteikšanas un reaģēšanas risinājumus (EDR) un SIEM telemetriju.

3.5 Ievērot tiesību aktu, regulatīvās un standartu prasības, kas nosaka galiekārtu drošību (piemēram, GDPR 32. pants, NIS2 21. pants, DORA 9. pants).

3.6 Noteikt atbildīgās lomas, ieviest ielāpu uzstādīšanas un reaģēšanas uz brīdinājumiem pakalpojumu līmeņa vienošanās (SLA), kā arī nodrošināt gatavību auditam ar dokumentācijas un ziņošanas palīdzību.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 ir šīs politikas īpašnieks un nodrošina tās saskaņotību ar IDPS un kopējo drošības stratēģiju;

4.1.2 reizi ceturksnī pārskata galiekārtu aizsardzības metriku, incidentu tendences un rīku efektivitāti;

4.1.3 apstiprina izņēmumus un atlikušā riska pieņemšanu, kas saistīta ar galiekārtu pārklājumu.

4.2 Galiekārtu drošības vadītājs/SOC vadītājs

4.2.1 pārvalda galiekārtu aizsardzības sistēmas (piemēram, AV, EDR, MDM);

4.2.2 pārrauga politikas ievērošanu, apdraudējumu noteikšanas regulēšanu un reaģēšanas rokasgrāmatas;

4.2.3 uztur pārklājuma statistiku, ļaunatūras incidentu žurnālus un brīdinājumu konfigurācijas pamatlīmeni.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata reizi gadā vai gadījumos, kad:

9.1.1 notiek nozīmīgas ļaunatūras kampaņas vai galiekārtu drošības incidenti;

9.1.2 jauni apdraudējumu veidi (piemēram, bezfailu ļaunatūra, izspiedējprogrammatūras varianti) prasa atjauninātas noteikšanas vai reaģēšanas stratēģijas;

9.1.3 būtiski mainās galiekārtu aizsardzības platformas vai aģentu arhitektūra;

9.1.4 tiek atjauninātas tiesību aktu vai regulatīvās prasības, kas ietekmē galiekārtu kontroles pasākumus.

9.2 Pārskatīšanu ierosina Galiekārtu drošības vadītājs un koordinē ar CISO, juridisko un atbilstības, risku un audita funkcijām.

9.3 Apstiprinātie grozījumi jādokumentē IDPS dokumentu kontroles reģistrā, tiem jāpiešķir jauns versijas identifikators un tie jāpaziņo visām skartajām pusēm.

9.4 Aizstātās versijas jāarhivē, piekļuve tām jāierobežo, un tās jāglabā audita pēdas integritātes nodrošināšanai saskaņā ar IDPS glabāšanas grafikiem.

10. Saistītās politikas un sasaiste

10.1 P1 - Informācijas drošības politika. Tā nosaka pamatprincipus sistēmu, datu un tīklu aizsardzībai. Šī politika īsteno minētos principus galiekārtu līmenī, izmantojot tehniskos un procesu kontroles pasākumus pret ļaunatūru.

10.2 P4 - Piekļuves kontroles politika. Tā nosaka lietotāju piekļuves ierobežojumus, kas tiek piemēroti galiekārtu līmenī, tostarp aizsardzību pret privilēģiju paaugstināšanu un nepārbaudītas programmatūras nesankcionētu uzstādīšanu.

10.3 P5 - Izmaiņu pārvaldības politika. Tā nodrošina, ka galiekārtu aizsardzības programmatūras, politikas noteikumu vai aģentu konfigurāciju atjauninājumiem tiek piemēroti apstiprināšanas un kontrolētas ieviešanas procesi.

10.4 P12 - Aktīvu pārvaldības politika. Tā nodrošina aktīvu klasifikācijas un uzskaites pamatlīmeni, kas nepieciešams galiekārtu pārskatāmībai, ielāpu pārklājumam un aizsardzības pret ļaunatūru piemērošanas jomas noteikšanai.

10.5 P22 - Žurnālfiksēšanas un uzraudzības politika. Tā nodrošina galiekārtu brīdinājumu, aģentu darbspējas statusa un draudu izlūkošanas integrāciju centralizētās SIEM sistēmās reāllaika noteikšanai un kriminālistiskajai izsekojamībai.

10.6 P30 - Incidentu reaģēšanas politika. Tā sasaista galiekārtās balstītus ļaunatūras incidentus ar standartizētām ierobežošanas, izskaušanas, izmeklēšanas un atjaunošanas darbplūsmām ar noteiktām lomām un eskalācijas sliekšņiem.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:

11.1.1 8. punkts - Darbības plānošana un kontrole: prasa ieviest tehniskos kontroles pasākumus, tostarp galiekārtu aizsardzības pasākumus, lai uzturētu IDPS mērķus.

11.2 ISO/IEC 27002:2022 - 8.7. un 8. kontroles pasākumi:

11.2.1 nosaka detalizētas tehniskās vadlīnijas pasākumiem pret ļaunprogrammatūru, drošai programmatūras ieviešanai, uzraudzībai un gatavībai incidentiem galiekārtu vidēs.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Aizsardzība pret ļaunprātīgu kodu: prasa izmantot aizsardzības rīkus pret ļaunatūru ar skenēšanu reāllaikā, skenēšanu piekļuves brīdī un uzvedības analīzi.

11.3.2 SI-4 - Sistēmu uzraudzība: atbalsta telemetrijas integrāciju ar centralizētām noteikšanas platformām.

11.3.3 CM-6 - Konfigurācijas iestatījumi: nostiprina pamatlīmeņa kontroles iestatījumus galiekārtās, tostarp aizsardzības aģentu obligātu piemērošanu.

11.4 ES GDPR (2016/679):

11.4.1 32. pants - apstrādes drošība: prasa organizācijām ieviest atbilstošus tehniskos pasākumus personas datu aizsardzībai, tostarp aizsardzību pret ļaunatūras apdraudējumiem.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 21. panta 2. punkta d) apakšpunkts: uzliek pienākumu ieviest apdraudējumu noteikšanas un novēršanas pasākumus, tostarp aizsardzības mehānismus pret ļaunatūru galiekārtu līmenī.

11.6 ES DORA (2022/2554):

11.6.1 9. pants - IKT risku pārvaldības prasības: prasa finanšu iestādēm ieviest aizsardzības pasākumus, lai novērstu, noteiktu un apstrādātu ļaunatūru un no galiekārtām izrietošus apdraudējumus.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Aizsardzība pret ļaunatūru: nosaka pienākumu nodrošināt ļaunatūras noteikšanu un mazināšanu visās organizācijas galiekārtās.

11.7.2 DSS01.04 - Pieejamības un kapacitātes pārvaldība: nodrošina, ka aizsardzība pret ļaunatūru ir sabalansēta ar sistēmu veiktspēju un darbības nepārtrauktību.

11.7.3 MEA03 - Atbilstības uzraudzība, izvērtēšana un novērtēšana: prasa periodisku galiekārtu kontroles pasākumu un aizsardzības efektivitātes auditu.