					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P20S					Dokumenta nosaukums: **Galapunktu aizsardzības pret ļaunatūru 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**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. nodaļa	Darbības kontroles pasākumi aizsardzībai pret ļaunatūru
ISO/IEC 27002:2022	8. kontrole	Galapunktu aizsardzības kontroles pasākumi
NIST SP 800-53 Rev.5	SI-3, SI-4	Aizsardzība pret ļaunprātīgu kodu un reaģēšana uz incidentiem
ES NIS2	21. panta 2. punkta d) un e) apakšpunkts	Aizsardzība pret ļaunatūru un risku pārvaldība būtiskām un svarīgām struktūrām
ES DORA	10. panta 1. punkts, 15. pants	Operacionālā noturība un trešo pušu verifikācija
COBIT 2019	DSS05.02, DSS05.04	Galapunktu un tīkla aizsardzība un uzraudzība
ES GDPR	32. panta 1. punkta b) apakšpunkts, 33. pants	Tehniskie un organizatoriskie pasākumi un paziņošana par pārkāpumu

1. Mērķis

1.1 Šī politika nosaka minimālās tehniskās, procesuālās un uzvedības prasības visu galapunkta ierīču, piemēram, klēpjdatoru, galddatoru, mobilo ierīču un pārnēsājamu datu nesēju, aizsardzībai pret ļaunprātīgu kodu, tostarp vīrusiem, izspiedējprogrammatūru, spiegprogrammatūru, rootkit tipa ļaunatūru un citiem ļaunatūras apdraudējumiem.

1.2 Tās mērķis ir nodrošināt, ka galapunkti ir aprīkoti, uzturēti un lietoti tā, lai samazinātu ļaunatūras inficēšanās, izplatīšanās un sistēmu kompromitēšanas risku.

1.3 Organizācija atzīst, ka galapunkti ir bieži sastopami ļaunatūras iekļuves punkti, tādēļ tie ir jācietina, jāuzrauga un jāaizsargā, izmantojot daudzslāņu aizsardzību.

1.4 Politika atbalsta organizācijas ISO/IEC 27001:2022 sertifikācijas mērķus un ir saskaņota ar Vispārīgo datu aizsardzības regulu (GDPR), NIS2 direktīvu, Digitālās darbības noturības aktu (DORA) un citiem piemērojamiem ietvariem.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem organizācijas galapunktiem, tostarp galddatoriem, klēpjdatoriem, planšetdatoriem, mobilajiem tālruņiem un tirdzniecības vietu terminālļiem;

2.1.2 personīgajām ierīcēm (BYOD), ko izmanto piekļuvei biznesa lietojumprogrammām vai datiem;

2.1.3 noņemamiem datu nesējiem, piemēram, USB datu nesējiem un ārējiem cietajiem diskiem;

2.1.4 jebkurām operētājsistēmām, galapunktu programmatūrai vai saziņas rīkiem, kas darbojas šajās platformās.

2.2 Tā vienlīdz attiecas uz:

2.2.1 iekšējo personālu, līgumdarbiniekiem, praktikantiem un pārvaldīto pakalpojumu sniedzējiem (MSP);

2.2.2 ierīcēm, ko izmanto klātienē, attālināti vai hibrīddarba režīmā;

2.2.3 ar mākoņpakalpojumiem savienotiem vai bezsaistes galapunktiem, kuros tiek glabāti biznesa dati vai personas dati.

3. Mērķi

3.1 Novērst ļaunatūras inficēšanos un izplatīšanos iekšējās sistēmās, lietotāju ierīcēs un ārējos savienojumos.

3.2 Savlaicīgi atklāt un ierobežot ar ļaunatūru saistītus apdraudējumus, izmantojot automatizētas galapunktu drošības tehnoloģijas un noteiktus eskalācijas ceļus.

3.3 Nodrošināt, ka piekļuve biznesa informācijai notiek tikai no autorizētām, aizsargātām un uzraudzītām ierīcēm.

3.4 Noteikt skaidrus personāla pienākumus un lietotāju uzvedības noteikumus, lai samazinātu ar ļaunatūru saistītu incidentu risku.

3.5 Uzturēt izsekojamus un auditējamus ierakstus par ļaunatūras atklāšanu, reaģēšanu un atbilstību šai politikai.

3.6 Aizsargāt personas datus un biznesa datus pret kompromitēšanu ļaunatūras dēļ, izmantojot daudzslāņu aizsardzības stratēģijas.

4. Lomas un pienākumi

4.1 Ģenerāldirektors

4.1.1 ir šīs politikas īpašnieks un nodrošina pietiekamu resursu pieejamību galapunktu aizsardzībai;

4.1.2 apstiprina pretvīrusu programmatūru, mobilo ierīču pārvaldības (MDM) rīkus un trešo pušu piekļuves noteikumus;

4.1.3 pārskata ar galapunktiem saistīto ļaunatūras incidentu pārskatus, ietekmes kopsavilkumus un paziņojumus par pārkāpumiem.

4.2 IT atbalsta pakalpojumu sniedzējs / iekšējais IT administrators

4.2.1 izvēlas un ievieš pretvīrusu programmatūru, aizsardzības pret ļaunatūru risinājumus un galapunktu atklāšanas un reaģēšanas (EDR) risinājumus;

4.2.2 nodrošina konsekventu atjauninājumu ieviešanu un žurnālu glabāšanu;

4.2.3 reaģē uz ļaunatūras brīdinājumiem, izolē inficētās sistēmas un veic novēršanas pasākumus;

4.2.4 ievieš kontroles pasākumus USB ierīču un ārējo ierīču lietošanai.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējās pārskatīšanas prasība

9.1.1 Šī politika vismaz reizi gadā formāli jāpārskata ģenerāldirektoram sadarbībā ar IT atbalsta pakalpojumu sniedzēju un privātuma koordinatoru.

9.2 Notikumu izraisīti atjauninājumi

9.2.1 Politika jāatjaunina arī tad, ja:

9.2.1.1 jauns būtisks ļaunatūras apdraudējums vai uzliesmojums ir vērsts pret organizācijas izmantotajiem galapunktiem;

9.2.1.2 pretvīrusu vai EDR rīki tiek mainīti, uzlaboti vai aizstāti;

9.2.1.3 ļaunatūras incidents atklāj nepilnības šīs politikas piemērošanas jomā vai ieviešanā;

9.2.1.4 tiek atjauninātas tiesiskās vai regulatīvās prasības (piemēram, GDPR, DORA, NIS2).

9.3 Versiju kontrole un informēšana

9.3.1 Visi politikas grozījumi jādokumentē, norādot versijas numuru, datumu un grozījumu kopsavilkumu.

9.3.2 Personāls jāinformē par atjauninājumiem, īpaši, ja tie maina darbības vai uzvedības prasības.

9.3.3 Iepriekšējās versijas jāsaglabā politikas arhīvā vismaz 3 gadus, lai nodrošinātu atbalstu auditiem.

10. Saistītās politikas un sasaiste

10.1 Šī politika jāievieš kopā ar šādām SME politikām:

10.1.1 P9S – Attālinātā darba politika: nodrošina, ka galapunktu aizsardzības prasības tiek piemērotas ierīcēm, ko izmanto ārpus organizācijas telpām vai hibrīddarba režīmā;

10.1.2 P12S – Aktīvu pārvaldības politika: atbalsta visu galapunktu uzskaiti un kontroli, nodrošinot, ka tiek izmantotas tikai autorizētas un aizsargātas ierīces;

10.1.3 P17S – Datu aizsardzības un privātuma politika: nostiprina ļaunatūras novēršanu kā būtisku privātuma kontroles pasākumu personas datu un sensitīvu datu aizsardzībai pret kompromitēšanu;

10.1.4 P22S – Žurnālfiksēšanas un uzraudzības politika: nosaka prasības ļaunatūras notikumu žurnālfiksēšanai un brīdinājumu redzamības uzturēšanai agrīnai reaģēšanai;

10.1.5 P30S – Incidentu pārvaldības politika: nosaka eskalācijas, ierobežošanas un ārējās paziņošanas darbības, ja ļaunatūra izraisa datu kompromitēšanu vai darbības traucējumus.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. nodaļa – prasa ieviest darbības kontroles pasākumus, lai mazinātu tādus riskus kā ļaunatūras uzbrukumi.

11.2 ISO/IEC 27002

11.2.1 8.7. kontrole – apraksta aizsardzības pret ļaunatūru praksi, tostarp pretvīrusu programmatūru, skenēšanu reāllaikā, atjauninājumus un lietotāju apmācību.

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – prasa ieviest aizsardzības mehānismus pret ļaunprātīgu kodu visos galapunktos.

11.3.2 SI-4 – nosaka uzraudzības, atklāšanas, analīzes un reaģēšanas darbības galapunkta līmeņa apdraudējumiem un brīdinājumiem.

11.4 ES GDPR

11.4.1 32. panta 1. punkta b) apakšpunkts – prasa tehniskos un organizatoriskos kontroles pasākumus (piemēram, pretvīrusu programmatūru) personas datu aizsardzībai.

11.4.2 33. pants – nosaka pienākumu paziņot par pārkāpumu, ja ļaunatūra apdraud datu integritāti, konfidencialitāti vai pieejamību.

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta d) apakšpunkts – prasa pasākumus ļaunatūras apdraudējumu novēršanai un reaģēšanai uz tiem būtiskās un svarīgās struktūrās.

11.5.2 21. panta 2. punkta e) apakšpunkts – nosaka daudzslāņu kiberdrošības risku pārvaldības stratēģijas, tostarp galapunktu aizsardzību pret ļaunatūru.

11.6 ES DORA

11.6.1 10. panta 1. punkts – prasa aizsargāt IKT sistēmas pret ļaunatūru un citiem apdraudējumiem kā daļu no operacionālās noturības.

11.6.2 15. pants – uzliek finanšu organizācijām pienākumu pārbaudīt aizsardzību pret ļaunatūru trešo pušu pakalpojumu sniedzēju vidē.

11.7 COBIT 2019

11.7.1 DSS05.02 – uzsver aizsardzības pasākumus galapunktu un tīklu aizsardzībai pret ļaunatūras apdraudējumiem.

11.7.2 DSS05.04 – atbalsta uzraudzību un brīdināšanu par ar ļaunatūru saistītiem drošības notikumiem nepārtrauktas darbības ietvaros.