					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P19					Dokumenta nosaukums: **Ievainojamību un ielāpu pārvaldības 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	Sistēmiska tehnisko ievainojamību apstrāde; drošības kontroles pasākumu nepārtraukta efektivitāte.
ISO/IEC 27002:2022	Kontroles pasākumi 8.8, 8.9, 5	Ieviešanas vadlīnijas ielāpu uzstādīšanai, ievainojamību skenēšanai, programmatūras integritātei, drošai konfigurācijai un aktīvu uzskaitei.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Tiek nodrošināta regulāra skenēšana, trūkumu novēršana un konfigurācijas pārvaldība.
ES VDAR	32. pants, 49. apsvērums	Tehniskie pasākumi savlaicīgai ielāpu uzstādīšanai, ievainojamību apstrādei un drošības nepārtrauktībai.
ES NIS2	21. panta 2. punkta d) apakšpunkts	Ievainojamību noteikšana, reaģēšana un mazināšana augsta kiberdrošības higiēnas līmeņa nodrošināšanai.
ES DORA	8. pants, 10. panta 2. punkta f) apakšpunkts	Savlaicīga IKT ievainojamību novēršana; nepārtraukta uz draudiem balstīta izvērtēšana.
COBIT 2019	DSS05.02, DSS01.03, MEA	Tehnisko vājo vietu skenēšana, izsekošana un mazināšana; uzraudzība, lai noteiktu izmantošanas mēģinājumus; efektivitātes audits, tostarp ielāpu statusa pārbaude.

1. Mērķis

1.1 Šī politika nosaka organizācijas obligātās prasības tehnisko ievainojamību un programmatūras trūkumu identificēšanai, klasificēšanai, novēršanai un uzraudzībai visās informācijas sistēmās un aktīvos, kas ietilpst informācijas drošības pārvaldības sistēmas (IDPS) tvērumā.

1.2 Tā nodrošina, ka visas zināmās ievainojamības tiek izvērtētas un novērstas savlaicīgi un uz risku balstītā veidā, izmantojot koordinētu ielāpu uzstādīšanu, konfigurācijas pielāgojumus vai kompensējošus kontroles pasākumus atbilstoši darbības vajadzībām un atbilstības pienākumiem.

1.3 Šī politika atbalsta atbilstību ISO/IEC 27001 A pielikuma 8. kontrolei un ISO/IEC 27002 vadlīnijām, kā arī aptver normatīvās prasības saskaņā ar DORA 8. pantu, NIS2 21. pantu, VDAR 32. pantu un COBIT 2019 DSS un APO jomām.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām informācijas sistēmām, aktīviem un vidēm, kurās tiek glabāti, apstrādāti vai pārsūtīti dati, uz kuriem attiecas IDPS pārvaldība, tostarp:

2.1.1 operētājsistēmām, lietotnēm, tīkla ierīcēm, aparātprogrammatūrai, mākoņplatformām, API un trešo pušu programmatūrai.

2.1.2 sistēmām izstrādes, testēšanas, ražošanas, rezerves kopiju un avārijas atjaunošanas vidēs.

2.1.3 galapunktiem, serveriem, IoT ierīcēm, virtualizācijas infrastruktūrai un konteineriem.

2.2 Tā ir saistoša:

2.2.1 iekšējam personālam: IT administratoriem, sistēmu inženieriem, lietotņu izstrādātājiem, drošības analītiķiem un infrastruktūras komandām.

2.2.2 ārējām pusēm: līgumslēdzējiem, trešo pušu pakalpojumu sniedzējiem, pārvaldīto pakalpojumu sniedzējiem (MSP), programmatūras piegādātājiem un sistēmu integratoriem, kuriem ir tehniski pienākumi attiecībā uz piemērošanas jomā esošajiem aktīviem.

2.3 Politika aptver pilnu ievainojamību un ielāpu dzīves ciklu, tostarp:

2.3.1 skenēšanu un noteikšanu

2.3.2 riska klasificēšanu un prioritāšu noteikšanu

2.3.3 ielāpu iegūšanu, testēšanu, ieviešanu un atcelšanu

2.3.4 izņēmumu pārvaldību un kompensējošo kontroles pasākumu plānošanu

2.3.5 žurnalēšanu, ziņošanu un audita izsekojamību

3. Mērķi

3.1 Nodrošināt, ka visas zināmās ievainojamības tiek identificētas, izvērtētas un novērstas tādā veidā, kas samazina pakļautību riskam un atbilst darbības prioritātēm.

3.2 Izveidot konsekventus, visā organizācijā vienotus procesus ievainojamību skenēšanai, būtiskuma klasificēšanai (piemēram, CVSS) un ielāpu pārvaldībai, tostarp ārkārtas apstrādei un atcelšanas plānošanai.

3.3 Nodrošināt drošas konfigurācijas pārvaldību, to saskaņojot ar drošās konfigurēšanas bāzlīmeņiem, izmaiņu pārvaldības praksi un reāllaika draudu izlūkošanu.

3.4 Nodrošināt izmērāmu atbilstību normatīvajām prasībām un standartos noteiktajiem kontroles pasākumiem, kas saistīti ar sistēmu integritāti, ielāpu higiēnu un savlaicīgu trūkumu novēršanu.

3.5 Noteikt atbildību un pārskatatbildību starp lomām visā ievainojamību pārvaldības dzīves ciklā, nodrošinot, ka visas iesaistītās puses darbojas saskaņā ar noteiktajām pakalpojumu līmeņa vienošanām (SLA) un ziņojamajiem kontroles pasākumu rādītājiem.

3.6 Veicināt gatavību auditam un uzlabot noturību pret jauniem apdraudējumiem, tostarp nulles dienas ievainojamībām, aktīvām izmantošanas ķēdēm un būtiskiem piegādātāju paziņojumiem.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 Atbild par šo politiku un nodrošina tās integrāciju IDPS.

4.1.2 Nosaka organizācijas riska apetīti un nodrošina saskaņotību ar normatīvajām prasībām un kontroles pasākumiem.

4.2 Ievainojamību pārvaldības vadītājs / drošības operāciju vadītājs

4.2.1 Pārrauga ievainojamību un ielāpu pārvaldības darbības pilnā apjomā.

4.2.2 Koordinē skenēšanas grafikus, prioritāšu noteikšanas modeļus un trūkumu novēršanas termiņus.

4.2.3 Uztur ievainojamību reģistru un sadarbojas kompensējošo kontroles pasākumu izvērtēšanā.

[... 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 vismaz reizi gadā vai pēc:

9.1.1 būtiskiem normatīvo prasību atjauninājumiem (piemēram, izmaiņām DORA, NIS2)

9.1.2 izmaiņām ievainojamību prioritāšu noteikšanas ietvarā (piemēram, CVSS atjauninājumiem)

9.1.3 būtiskām IT vides izmaiņām (piemēram, migrācijas uz mākoņvidi, EDR risinājuma būtiskas pārbūves)

9.1.4 nozīmīgiem pārkāpumiem vai ārējiem paziņojumiem, kuru dēļ nepieciešams stiprināt politiku

9.2 Pārskatīšanu veic CISO sadarbībā ar drošības operācijām, risku pārvaldību un infrastruktūras vadību.

9.3 Politikas atjauninājumiem jābūt:

9.3.1 dokumentētiem IDPS dokumentu kontroles reģistrā

9.3.2 pārskatītiem un apstiprinātiem izpildvadībā

9.3.3 paziņotiem visām skartajām iesaistītajām pusēm, tostarp trešo pušu apstrādātājiem

9.4 Vēsturiskās versijas droši jāglabā audita un pārskatatbildības vajadzībām.

10. Saistītās politikas un sasaiste

10.1 P1 - Informācijas drošības politika. Tā nosaka vispārējo apņemšanos aizsargāt sistēmas un datus, tostarp proaktīvu ievainojamību pārvaldību un programmatūras integritātes nodrošināšanu.

10.2 P5 - Izmaiņu pārvaldības politika. Tā regulē visu ielāpu ieviešanu un konfigurācijas pielāgojumus, nosakot dokumentēšanas, testēšanas, apstiprināšanas un atcelšanas procedūras, kas papildina ievainojamību novēršanas procesus.

10.3 P6 - Risku pārvaldības politika. Tā atbalsta nenovērstu ievainojamību klasificēšanu un riska apstrādi, izmantojot strukturētu risku izvērtēšanu, ietekmes analīzi un atlikušā riska pieņemšanas procedūras.

10.4 P12 - Aktīvu pārvaldības politika. Tā nodrošina, ka sistēmas tiek precīzi uzskaitītas un klasificētas, tādējādi ļaujot veikt konsekventu ievainojamību skenēšanu, īpašnieku noteikšanu un ielāpu piemērošanu visā dzīves ciklā.

10.5 P22 - Žurnalēšanas un uzraudzības politika. Tā nosaka prasības notikumu noteikšanai un audita pēdas izveidei. Šī politika nodrošina redzamību par ielāpu uzstādīšanas darbībām, nesankcionētām izmaiņām un zināmām ievainojamībām vērstiem izmantošanas mēģinājumiem.

10.6 P30 - Incidentu reaģēšanas politika. Tā nosaka eskalācijas protokolus un ierobežošanas stratēģijas izmantotu ievainojamību, pārkāpumu izmeklēšanas un korektīvo darbību gadījumiem atbilstoši šīs politikas kontroles pasākumiem.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:2022 8.1. punkts - darbības plānošana un kontrole: nosaka prasību sistemātiski apstrādāt tehniskās ievainojamības, lai nodrošinātu drošības kontroles pasākumu nepārtrauktu efektivitāti.

11.2 ISO/IEC 27002:2022 - kontroles pasākumi 8.8, 8.9, 5: sniedz ieviešanas vadlīnijas ielāpu uzstādīšanai, ievainojamību skenēšanai, programmatūras integritātei un integrācijai ar drošu konfigurāciju un aktīvu uzskaiti.

11.3 NIST SP 800-53 Rev.5: RA-5 - ievainojamību uzraudzība un skenēšana: nosaka regulāru skenēšanu un trūkumu novēršanas izsekošanu. SI-2 - trūkumu novēršana: prasa savlaicīgu trūkumu izvērtēšanu un mazināšanu, izmantojot pieejamos ielāpus vai citas darbības. CM-2 / CM-6 - konfigurācijas pārvaldības bāzlīmeņi un kontroles pasākumi: nosaka drošu sistēmu konfigurāciju pamatu, kas ir sasaistīts ar ielāpu ieviešanu.

11.4 ES VDAR (2016/679): 32. pants - apstrādes drošība: prasa ieviest atbilstošus tehniskos pasākumus, piemēram, savlaicīgu ielāpu uzstādīšanu un ievainojamību apstrādi, lai nodrošinātu

konfidencialitāti un sistēmu noturību. 49. apsvērums: mudina organizācijas ieviest preventīvus kontroles pasākumus pret zināmiem apdraudējumiem, lai atbalstītu drošību un nepārtrauktību.

11.5 ES NIS2 direktīva (2022/2555): 21. panta 2. punkta d) apakšpunkts: uzliek par pienākumu būtiskajām un svarīgajām vienībām noteikt, apstrādāt un mazināt sistēmu ievainojamības un uzturēt augstu kiberdrošības higiēnas līmeni.

11.6 ES DORA (2022/2554): 8. pants - IKT risku pārvaldība: prasa identificēt un savlaicīgi novērst ievainojamības informācijas un komunikācijas tehnoloģijās, ko izmanto finanšu sistēmās. 10. panta 2. punkta f) apakšpunkts: uzsver nepārtrauktas uz draudiem balstītas ievainojamību izvērtēšanas un ielāpu uzstādīšanas nozīmi kā darbības noturības daļu.

11.7 COBIT 2019: DSS05.02 - drošības ievainojamību pārvaldība: nosaka organizācijām skenēt, izsekot un mazināt zināmās tehniskās vājās vietas. DSS01.03 - infrastruktūras uzraudzība: nodrošina, ka sistēmas tiek uzraudzītas, lai noteiktu izmantošanas pazīmes vai vājās vietas. MEA03 - atbilstības uzraudzība, izvērtēšana un novērtēšana: prasa regulāru kontroles pasākumu efektivitātes auditu, tostarp ielāpu statusa un izņēmumu pārvaldības pārbaudi.