					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P19S					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**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	
ISO/IEC 27002:2022	8.8, 8. nodaļas kontroles pasākumi	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
ES NIS2	21. panta 2. punkta d) un e) apakšpunkts	
ES DORA	8. panta 1. punkts, 10. panta 2. punkts	
COBIT 2019	DSS05.02, APO12	
ES VDAR	32. panta 1. punkta b) apakšpunkts	

1. Mērķis

1.1 Šī politika nosaka, kā organizācija identificē, novērtē un mazina ievainojamības sistēmās, lietojumprogrammās un infrastruktūrā.

1.2 Tās mērķis ir samazināt kiberdrošības risku, nodrošinot savlaicīgu ielāpu ieviešanu un uz risku balstītu trūkumu novēršanas praksi, kas ir piemērota mazajiem un vidējiem uzņēmumiem (SME).

1.3 Šī politika atbalsta atbilstību ISO/IEC 27001:2022 sertifikācijas prasībām un palīdz izpildīt VDAR, NIS2 un DORA noteiktos regulatīvos pienākumus, paredzot proaktīvu tehnisko ievainojamību pārvaldību.

1.4 Organizācija atzīst, ka neielāpītas sistēmas rada būtisku apdraudējumu informācijas drošībai un ir sistemātiski un bez kavēšanās jānovērš.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem serveriem, galddatoriem, portatīvajiem datoriem, mobilajām ierīcēm, tīkla iekārtām un mākoņvidē izvietotām platformām, ko izmanto organizācija;

2.1.2 visām operētājsistēmām, trešo pušu programmatūru, spraudņiem un lietojumprogrammām, ko izmanto biznesa procesos;

2.1.3 iekšējo IT personālu un ārējiem pakalpojumu sniedzējiem, kuri ir atbildīgi par sistēmu uzturēšanu, atjaunināšanu vai uzraudzību;

2.1.4 jebkuru individuāli izstrādātu pirmkodu vai iegulto programmatūru, ko uztur organizācija vai kas tiek uzturēta tās vārdā.

2.2 Politika aptver gan infrastruktūru, ko organizācija pārvalda tieši, gan sistēmas, ko administrē nolīgtie piegādātāji vai mitināšanas pakalpojumu sniedzēji.

3. Mērķi

3.1 Savlaicīgi un konsekventi identificēt un novērtēt zināmās ievainojamības visos IT aktīvos.

3.2 Piemērot ielāpus un programmatūras atjauninājumus, pamatojoties uz smaguma pakāpi un risku organizācijas darbībai vai personas datiem.

3.3 Novērst tehnisko vājību izmantošanu, kas var izraisīt pakalpojumu darbības traucējumus, personas datu aizsardzības pārkāpumu vai neatbilstību tiesiskajām prasībām.

3.4 Uzturēt precīzus ierakstus par uzstādītajiem ielāpiem, neatrisinātajiem jautājumiem un izņēmumiem, lai nodrošinātu gatavību auditam.

3.5 Izmantot organizācijas lielumam un darbības sarežģītībai atbilstošus rīkus un procesus, nepasliktinot efektivitāti.

3.6 Atbalstīt tiesisko un regulatīvo atbilstību, tostarp VDAR 32. pantam un ISO A pielikuma 8. kontrolei.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 ir vispārīgi atbildīgs par to, lai tiktu ieviestas ielāpu pārvaldības un ievainojamību pārvaldības darbības;

4.1.2 apstiprina riska izņēmumus gadījumos, kad ielāpus nav iespējams uzstādīt, un pārskata saistītās riska mazināšanas stratēģijas;

4.1.3 pārskata ziņojumus par ielāpu statusu un nodrošina resursu pieejamību ielāpu pārvaldības pienākumu izpildei.

4.2 IT atbalsta pakalpojumu sniedzējs / iekšējais IT administrators

4.2.1 uzrauga sistēmas attiecībā uz ievainojamībām un pieejamajiem ielāpiem, izmantojot piegādātāju brīdinājumus, draudu paziņojumus un operētājsistēmu līmeņa paziņojumus;

4.2.2 piemēro operētājsistēmu, aparātprogrammatūras un lietojumprogrammu atjauninājumus noteiktajos termiņos;

4.2.3 uztur formālu ielāpu žurnālu un dokumentē neatrisinātos vai atliktos atjauninājumus;

4.2.4 veic kritisko atjauninājumu testēšanu un plānošanu, lai mazinātu darbības traucējumus.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējā pārskatīšana

9.1.1 Šī politika jāpārskata vismaz reizi gadā ģenerāldirektoram, saņemot ieguldījumu no IT pakalpojumu sniedzēja un privātuma koordinatora.

9.2 Pārskatīšanas ierosinātāji

9.2.1 Starpposma pārskatīšana jāveic, ja:

9.2.1.1 būtiska ievainojamība vai izmantošanas paņēmiens ietekmē piemērošanas jomā ietvertās sistēmas;

9.2.1.2 notiek nozīmīgas sistēmu vai programmatūras izmaiņas;

9.2.1.3 audits konstatē trūkumus ielāpu pārvaldības procesos;

9.2.1.4 tiek reģistrēts ar ielāpu pārvaldību saistīts incidents vai pārkāpums.

9.3 Politikas versiju kontrole

9.3.1 Visi atjauninājumi jāreģistrē versiju žurnālā, ietverot izmaiņu kopsavilkumu.

9.3.2 Izmaiņas jāpaziņo skartajam personālam.

9.3.3 Novecojušās versijas jāarhivē ar ierobežotu piekļuvi.

10. Saistītās politikas un sasaiste

10.1 Šī politika atbalsta vairākas citas SME politikas un ir ar tām savstarpēji saistīta:

10.1.1 P12S – Aktīvu pārvaldības politika: nosaka sistēmu īpašumtiesības un klasifikāciju, nodrošinot, ka visi ielāpu uzstādīšanai pakļautie aktīvi ir uzskaitīti un iekļauti aktīvu reģistrā;

10.1.2 P14S – Datu glabāšanas un dzēšanas politika: nodrošina, ka sistēmas, kurām plānota izņemšana no ekspluatācijas, tiek droši atjauninātas vai dzēstas, tādējādi samazinot pakļautību ievainojamībām;

10.1.3 P17S – Datu aizsardzības un privātuma politika: piešķir prioritāti ievainojamību novēršanai sistēmās, kurās tiek apstrādāti personas dati, lai nodrošinātu atbilstību privātuma tiesību aktiem;

10.1.4 P22S – Žurnālfailu reģistrēšanas un uzraudzības politika: atbalsta neielāpītu sistēmu vai aizdomīgas uzvedības noteikšanu, kas var liecināt par ievainojamības izmantošanu;

10.1.5 P30S – Incidentu reaģēšanas politika: nosaka procedūras reaģēšanai uz ievainojamībām, kas izraisa drošības incidentus, tostarp eskalācijas un ziņošanas soļus.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts – paredz kontroles pasākumu ieviešanu darbības risku novēršanai, tostarp ievainojamību pārvaldībai.

11.2 ISO/IEC 27002

11.2.1 8.8 kontrole – nosaka procesus zināmu sistēmu vājību skenēšanai un novēršanai.

11.2.2 8.9 kontrole – uzsver drošu konfigurāciju, ielāpu validāciju un izmaiņu kontroli, lai atjauninājumu laikā nepieļautu jaunu pakļautību riskam.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – nosaka prasību identificēt ievainojamības un novērst tās noteiktajos termiņos.

11.3.2 SI-2 – nosaka pienākumu nekavējoties piemērot ielāpus un atjauninājumus atbilstoši smaguma pakāpei.

11.3.3 CM-2 – nosaka sistēmu bāzlīnijas konfigurācijas un atjauninājumu dokumentēšanas prasības, lai nodrošinātu konsekventus aizsardzības pasākumus.

11.4 ES VDAR

11.4.1 32. panta 1. punkta b) apakšpunkts – prasa organizācijām ieviest atbilstošus tehniskos pasākumus, tostarp ielāpu pārvaldību, lai nodrošinātu apstrādes drošību.

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta d) apakšpunkts – prasa ievainojamību pārvaldību, izmantojot sistemātisku skenēšanu un trūkumu novēršanu.

11.5.2 21. panta 2. punkta e) apakšpunkts – uzliek pienākumu nodrošināt drošu konfigurāciju un ielāpu pārvaldību, lai stiprinātu IKT noturību.

11.6 ES DORA

11.6.1 8. panta 1. punkts – prasa IKT risku noteikšanu un mazināšanu, tostarp tehnisko ievainojamību gadījumā.

11.6.2 10. panta 2. punkts – uzliek finanšu iestādēm pienākumu novērst vājības, kas ietekmē IKT sistēmas un darbību.

11.7 COBIT 2019

11.7.1 DSS05.02 – prasa apstrādāt zināmās tehniskās ievainojamības, lai uzturētu drošu darbību.

11.7.2 APO12.01 – saskaņo risku pārvaldību ar proaktīvu sistēmu vājību uzraudzību un novēršanu.