					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P39					Dokumenta nosaukums: **Koordinētas ievainojamību izpaušanas 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	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
ES VDAR	32. panta 1. punkta d) apakšpunkts	
ES NIS2	21. panta 2. punkta e) apakšpunkts	
ES DORA	11. panta 1. punkta d) apakšpunkts	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Mērķis

1.1 Noteikt formālu procesu ievainojamību informācijas saņemšanai, apstrādei un izpaušanai attiecībā uz ievainojamībām, kas ietekmē organizācijas sistēmas vai pakalpojumus, kā to nosaka NIS2 direktīvas 21. panta 2. punkta e) apakšpunkts par ievainojamību apstrādi un izpaušanu.

1.2 Veicināt ārējo drošības pētnieku, partneru un lietotāju atbildīgu ziņošanu par ievainojamībām (Coordinated Vulnerability Disclosure — CVD), kā arī noteikt, kā organizācija komunicē informāciju par ievainojamībām iesaistītajām pusēm.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām organizācijas īpašumā esošajām vai tās pārvaldītajām tīkla un informācijas sistēmām, kā arī uz jebkurām šajās sistēmās identificētajām ievainojamībām.

2.2 Tā attiecas uz iekšējām komandām (drošības, IT un izstrādes) un jebkurām ārējām pusēm, kas ziņo par ievainojamībām (piemēram, pētniekiem, klientiem, piegādātājiem). Tā reglamentē arī saziņu ar produktu piegādātājiem vai pakalpojumu sniedzējiem, ja ievainojamība skar to komponentes.

3. Mērķi

3.1 Savlaicīgi atklāt un novērst drošības ievainojamības, izmantojot gan iekšējo izvērtēšanu, gan ārēji saņemtu informāciju par ievainojamībām.

3.2 Nodrošināt skaidras vadlīnijas ārējiem ziņotājiem drošai un tiesiskai informācijas par ievainojamībām iesniegšanai, kā arī organizācijai efektīvai reaģēšanai un trūkumu novēršanai.

3.3 Nodrošināt atbilstību NIS2 prasībām un nozares labajai praksei (ISO/IEC 29147 un ISO/IEC 30111) koordinētas ievainojamību izpaušanas jomā, uzlabojot kopējo ekosistēmas drošību.

4. Lomas un pienākumi

4.1 Ievainojamību reaģēšanas komanda (VRT): norīkota komanda galvenā informācijas drošības vadītāja (CISO) vai ievainojamību pārvaldības vadītāja vadībā, kas saņem un sākotnēji izvērtē ievainojamību ziņojumus, novērtē risku un ietekmi, kā arī koordinē trūkumu novēršanu un publisku izpaušanu.

4.2 IT un izstrādes komandas: sadarbojas ar VRT, lai validētu ziņotās ievainojamības, izstrādātu un testētu ielāpus vai risku mazinošus drošības pasākumus un ieviestu labojumus. Pēc vajadzības sniedz tehnisko informāciju paziņojumu sagatavošanai.

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

9. Uzraudzība un audits

9.1 VRT uztur ievainojamību izpaušanas žurnālu, kurā tiek uzskaitīts katrs ziņojums no saņemšanas līdz slēgšanai. Šis žurnāls tiek pārskatīts reizi mēnesī, lai nodrošinātu savlaicīgu virzību atvērtajiem jautājumiem. Kavētie jautājumi jāeskalē.

9.2 Iekšējais audits vai neatkarīgs drošības izvērtētājs katru gadu pārskata ievainojamību apstrādes procesa efektivitāti, piemēram, pārbaudot, vai ievainojamību gadījumu izlase ir apstrādāta atbilstoši politikai, tostarp vai ir veikts saņemšanas apliecinājums, novēršana un izpaušana savlaicīgā termiņā. Tiek pārbaudīts arī, vai publiski pieejamais izpaušanas kanāls darbojas, piemēram, vai testa e-pasti tiek saņemti un uz tiem tiek reaģēts.

9.3 Metrikas par ievainojamībām, tostarp apjoms pēc smaguma pakāpes, trūkumu novēršanas laiki u. c., reizi ceturksnī tiek apkopotas un iesniegtas kiberdrošības pārvaldības komitejai, lai aktualizētu risku izvērtējumu.

10. Pārskatīšana un uzturēšana

10.1 Šī politika jāpārskata vismaz reizi gadā. Papildus tam ārpuskārtas pārskatīšanu izraisa jebkuras būtiskas izmaiņas IT vidē, piemēram, jauna internetam pieejama pakalpojuma ieviešana, vai būtiskas normatīvo prasību izmaiņas, piemēram, jauni ES tiesību akti par produktu ievainojamību izpaušanu.

10.2 Politikas atjauninājumos jāiekļauj ārējo ziņotāju atsauksmes un iekšējo pēcincidenta analīžu atziņas. Būtiskas izmaiņas apstiprina CISO, un par tām tiek informēti visi darbinieki; tās tiek arī publicētas organizācijas tiešsaistes drošības politiku repozitorijā pārredzamības nolūkos.

11. Saistītās politikas un sasaiste

11.1 P01 – Informācijas drošības politika. Vadības mandāts ievainojamību apstrādei un izpaušanai.

11.2 P19 – Ievainojamību un ielāpu pārvaldības politika. Iekšējais trūkumu novēršanas process, kas sasaistīts ar CVD ziņojumu pieņemšanu.

11.3 P24 – Drošas izstrādes politika. Nodrošina labojumu ieviešanu un programmatūras izstrādes dzīves cikla (SDLC) drošības stiprināšanu, balstoties uz ziņotajām problēmām.

11.4 P25 – Lietojumprogrammu drošības prasību politika. Nodrošina, ka produktiem ir izpaušanai gatavas drošības prasības.

11.5 P30 – Incidentu reaģēšanas politika. Aptver atklāti izmantotu ievainojamību aktīvu ekspluatāciju.

11.6 P31 – Digitālo pierādījumu iegūšanas un datorforensikas politika. Nodrošina artefaktu saglabāšanu no ziņotām vai izmantotām ievainojamībām.

11.7 P26 – Trešo pušu un piegādātāju drošības politika. Koordinē izpaušanu gadījumos, kad ievainojamība skar piegādātāju komponentes.

11.8 P37 – Juridisko jautājumu un regulatīvās atbilstības politika. Reglamentē paziņošanu, drošās ostas formulējumus un publikāciju.

12. Atsauces

12.1 NIS2 direktīva (ES 2022/2555), 21. panta 2. punkta e) apakšpunkts (drošība izstrādē un ievainojamību apstrāde un izpaušana)

12.2 Komisijas Īstenošanas regula (ES) 2024/2690, pielikuma 6.10. iedaļa (tehniskās prasības ievainojamību apstrādes un izpaušanas procesiem)

12.3 ENISA tehniskās vadlīnijas par kiberdrošības riska pārvaldības pasākumiem – sadaļa par ievainojamību apstrādi un izpaušanu

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontrole A.5.7 par draudu izlūkošanu un ievainojamību izpaušanu; kontrole A.8.28 par drošu izstrādi)

12.5 ISO/IEC 29147:2018 (vadlīnijas ievainojamību izpaušanai) un ISO/IEC 30111:2019 (vadlīnijas ievainojamību apstrādes procesiem)