					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P39					Dokumendi pealkiri: **Koordineeritud haavatavuste avalikustamise poliitika**						
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:						
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Kooskõla standardite ja regulatsioonidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
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	
ELi GDPR	art 32(1)(d)	
ELi NIS2	art 21(2)(e)	
ELi DORA	art 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Eesmärk

1.1 Kehtestada ametlik protsess organisatsiooni süsteeme või teenuseid mõjutavate haavatavuste kohta teabe vastuvõtmiseks, käsitlemiseks ja avalikustamiseks kooskõlas NIS2 artikli 21 lõike 2 punktiga e, mis käsitleb haavatavuste käsitlemist ja avalikustamist.

1.2 Julgustada väliseid turbeuurijaid, partnereid ja kasutajaid teatama haavatavustest vastutustundlikult koordineeritud haavatavuste avalikustamise (CVD) korras ning määratleda, kuidas organisatsioon edastab haavatavustega seotud teavet sidusrühmadele.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile organisatsiooni omanduses olevatele või hallatavatele võrgu- ja infosüsteemidele ning kõigile nendes süsteemides tuvastatud haavatavustele.

2.2 Poliitika hõlmab sisemisi meeskondi (turve, IT, arendus) ning kõiki väliseid osapooli, kes teatavad haavatavustest (nt uurijad, kliendid, tarnijad). Samuti reguleerib see teabevahetust tootjate või teenuseosutajatega, kui haavatavus puudutab nende komponente.

3. Eesmärgid

3.1 Tuvastada ja kõrvaldada turvanõrkused õigeaegselt, kasutades nii sisemisi hindamisi kui ka väliseid teavitusi.

3.2 Anda välistele teavitajatele selged juhised haavatavusteabe turvaliseks ja seaduslikuks esitamiseks ning organisatsioonile juhised tõhusaks reageerimiseks ja puuduste kõrvaldamiseks.

3.3 Tagada kooskõla NIS2 nõuete ja valdkonna heade tavadega (ISO/IEC 29147 ja ISO/IEC 30111) koordineeritud haavatavuste avalikustamisel ning tugevdada kogu ökosüsteemi turvalisust.

4. Rollid ja vastutused

4.1 Haavatavustele reageerimise meeskond (VRT): määratud meeskond, mida juhib infoturbe juht või haavatavuste halduse juht ning kes võtab vastu haavatavusteated, teeb nende triaaži, hindab riski ja mõju ning koordineerib puuduste kõrvaldamist ja avalikustamist.

4.2 IT- ja arendusmeeskonnad: teevad koostööd VRT-ga, et valideerida teatatud haavatavused, töötada välja ja testida turvaparandused või leevendusmeetmed ning juurutada parandused. Vajaduse korral esitavad nad teavituste koostamiseks tehnilised üksikasjad.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Seire ja audit

9.1 VRT peab pidama haavatavuste avalikustamise logi, milles jälgitakse iga teadet alates vastuvõtmisest kuni sulgemiseni. Seda logi vaadatakse läbi kord kuus, et tagada avatud juhtumite õigeaegne edenemine. Tähtaega ületanud juhtumid tuleb eskaleerida.

9.2 Siseaudit või sõltumatu turbehindaja vaatab kord aastas läbi haavatavuste käsitlemise protsessi tõhususe, näiteks kontrollides, kas valimit haavatavusjuhtumitest käsitleti vastavalt poliitikale (kättesaamine kinnitati, parandus tehti, teavitus avaldati õigeaegselt). Samuti kontrollitakse, et avalikult kättesaadav teavituskanal toimib (nt testkirjad võetakse vastu ja neile reageeritakse).

9.3 Haavatavuste mõõdikud (maht raskusastme järgi, parandamisajad jne) koostatakse kord kvartalis ja esitatakse küberturbe juhtkomiteele, et toetada riskihindamiste ajakohastamist.

10. Läbivaatamine ja hooldus

10.1 Käesolev poliitika vaadatakse läbi vähemalt kord aastas. Lisaks käivitab erakorralise läbivaatamise iga oluline muudatus meie IT-keskkonnas (nt uue internetti avatud teenuse kasutuselevõtt) või asjakohane regulatiivne areng (nt uued ELi õigusaktid toodete haavatavuste avalikustamise kohta).

10.2 Poliitika ajakohastamisel võetakse arvesse väliste teavitajate tagasisidet ja sisemistest intsidendijärgsetest analüüsidest saadud õppetunde. Olulised muudatused kiidab heaks infoturbe juht, neist teavitatakse kõiki töötajaid ning need avaldatakse läbipaistvuse tagamiseks organisatsiooni veebipõhises turbepoliitikate keskhoidlas.

11. Seotud poliitikad ja seosed

11.1 P01 – Infoturbepoliitika. Juhtkonna mandaat haavatavuste käsitlemiseks ja avalikustamiseks.

11.2 P19 – Haavatavuste ja paikade halduse poliitika. CVD sisendiga seotud sisemine puuduste kõrvaldamise töövoog.

11.3 P24 – Turvalise arenduse poliitika. Tagab teatatud juhtumitest tulenevate paranduste rakendamise ja SDLC tugevdamise.

11.4 P25 – Rakendusturbe nõuete poliitika. Tagab, et toodetel on avalikustamiseks valmis rakendusturbe nõuded.

11.5 P30 – Intsidentidele reageerimise poliitika (P30). Käsitleb avalikustatud haavatavuste aktiivset ärakasutamist.

11.6 P31 – Tõendite kogumise ja kohtuekspertiisi poliitika. Säilitab teatatud või ära kasutatud puudustega seotud artefaktid.

11.7 P26 – Kolmandate osapoolte ja tarnijate turbepoliitika. Koordineerib avalikustamisi, mis puudutavad tarnijate komponente.

11.8 P37 – Õiguse ja vastavuse poliitika. Reguleerib teavitamist, heauskse tegevuse kaitse sõnastust ja avaldamist.

12. Viited

12.1 NIS2 direktiiv (EL 2022/2555), artikli 21 lõike 2 punkt e (turvalisus arenduses ning haavatavuste käsitlemine ja avalikustamine)

12.2 Komisjoni rakendusmäärus (EL) 2024/2690, lisa punkt 6.10 (tehnilised nõuded haavatavuste käsitlemise ja avalikustamise protsessidele)

12.3 ENISA tehnilised suunised küberturbe riskijuhtimise meetmete kohta – haavatavuste käsitlemise ja avalikustamise osa

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (meede 5.7 ohuteabe ja haavatavuste avalikustamise kohta; meede 8.28 turvalise arenduse kohta)

12.5 ISO/IEC 29147:2018 (haavatavuste avalikustamise suunised) ja ISO/IEC 30111:2019 (haavatavuste käsitlemise protsesside suunised)