					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P30					Dokumendi pealkiri: **Intsidentidele reageerimise 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/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8.1, punkt 9	Struktureeritud protsessid riskijuhtimiseks ja intsidentidele reageerimiseks
ISO/IEC 27002:2022	Kontrollimeetmed 5.25–5.27	Intsidentidega seotud rollid, teavitamine, reageerimine ja täiustamine
NIST SP 800-53 Rev.5	IR-1 kuni IR-9	Intsidentidele reageerimise elutsükli terviklik käsitlus
EL GDPR	Artikkel 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Rikkumisest teatamise tähtajad, aruandlus ja andmesubjektide teavitamine
EL NIS2	Artikkel 23(1)–(4)	Pädeva asutuse teavitamine ja struktureeritud aruandlus
EL DORA	Artikkel 17(1)–(3)	Olulistest IKT-ga seotud intsidentidest teatamine finantssektori üksustes
COBIT 2019	DSS02, DSS04, MEA	Määratleb intsidendihalduse, talitluspidevuse, hindamise põhimõtted ja seire

1. Eesmärk

1.1 Käesolev poliitika kehtestab formaalse raamistiku organisatsiooni mõjutavate infoturbeintsidentide tuvastamiseks, neist teatamiseks, analüüsimiseks, ohjeldamiseks, neile reageerimiseks, taastamiseks ja intsidendijärgseks hindamiseks.

1.2 Poliitika eesmärk on tagada õigeaegne, koordineeritud ja tõhus reageerimine, et minimeerida tegevushäireid, rahalist kahju, mainekahju ja õigusnormidele mittevastavust.

1.3 Poliitika toetab ka organisatsiooni küberkerksuse pidevat täiustamist, kasutades saadud õppetunde ning sidudes intsidendijärgsed leiud juhtimise, töövahendite ja koolitusprogrammidega.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmistele osapooltele ja objektidele:

2.1.1 kogu personalile, sealhulgas töötajatele, töövõtjatele, konsultantidele ja kolmandatest osapooltest teenuseosutajatele;

2.1.2 kõigile infosüsteemidele, rakendustele, taristule, võrkudele ja andmetele sõltumata sellest, kas need asuvad kohapeal, pilvekeskkonnas või hübriidkeskkonnas;

2.1.3 kõigile turbeintsidentide liikidele, sealhulgas, kuid mitte ainult, järgmistele juhtumitele:

2.1.3.1 loata juurdepääs või õiguste laiendamine;

2.1.3.2 pahavara- ja lunavararünnakud;

2.1.3.3 teenusetõkestusrünnakud (DoS/DDoS);

2.1.3.4 andmekadu, andmeleke või andmete väljaviimine;

2.1.3.5 siseisikute väärkasutus või poliitikarikkumised;

2.1.3.6 füüsilise turbe rikkumised, mis mõjutavad digitaalseid varasid.

2.2 Poliitika hõlmab tuvastamist, triaaži, uurimist, eskaleerimist, ohjeldamist, tõendusmaterjali käitlemist, teavitamist, taastamist ja algpõhjuse analüüsi.

3. Eesmärgid

3.1 Luua korratav ja skaleeritav intsidentidele reageerimise võimekus, mis võimaldab turbeintsidente kiiresti tuvastada, klassifitseerida ja maandada.

3.2 Minimeerida turbesündmuste ärimõju struktureeritud ohjeldamise, kõrvaldamise ja süsteemide taastamise protseduuride kaudu.

3.3 Tagada, et intsidentidest teatamine ja neile reageerimine oleks kooskõlas õiguslike, regulatiivsete ja lepinguliste nõuetega, eelkõige rikkumisest teatamise tähtaegade ja tõendusmaterjali käitlemise osas.

3.4 Tagada läbipaistvus ja vastutus nõuetekohase logimise, dokumenteerimise ja mõõdikute jälgimise kaudu kõigi turbeintsidentide puhul.

3.5 Edendada pidevat täiustamist intsidendijärgsete läbivaatamiste, parandusmeetmete ja sidusrühmade koolitamise kaudu.

4. Rollid ja vastutused

4.1 infoturbejuht

4.1.1 Vastutab intsidentidele reageerimise raamistiku eest, tagab poliitika rakendamise ning teostab organisatsiooniülest järelevalvet intsidentide koordineerimise üle.

4.1.2 Täidab peamise kontaktisiku rolli regulaatorite, tippjuhtkonna ja välise õigusnõustajaga suhtlemisel suure mõjuga intsidentide korral.

4.2 Intsidentidele reageerimise koordinaator

4.2.1 Koordineerib valdkondadeüleseid reageerimismeeskondi, haldab töövooge ning jälgib ohjeldamise ja taastamise staatust.

4.2.2 Algatab ja juhib intsidendijärgseid ülevaatusi (PIR) ning tagab, et parandusmeetmed logitakse ja rakendatakse.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt kord aastas ja vajaduse korral ajakohastada, et võtta arvesse järgmist:

9.1.1 muudatused ohumaastikus, intsidentide liikides või ründevektorites;

9.1.2 suure mõjuga intsidentidest, peaaegu juhtumitest või regulatiivsetest leidudest saadud õppetunnid;

9.1.3 asjakohaste õigusaktide ja regulatsioonide muudatused (nt GDPR, DORA, NIS2);

9.1.4 tagasiside intsidentidele reageerimise õppustest ja intsidendijärgsetest läbivaatamistest.

9.2 infoturbejuht vastutab läbivaatamisprotsessi algatamise ja koordineerimise eest, konsulteerides järgmiste osapooltega:

9.2.1.1 õigusnõustaja ja andmekaitseametnik;

9.2.1.2 SOC ja IT-operatsioonid;

9.2.1.3 talitluspidevuse ja riskijuhtimise meeskonnad;

9.2.1.4 tippjuhtkond.

9.3 Poliitikamuudatused peavad olema:

9.3.1 dokumenteeritud versioonihaldusega repositooriumis;

9.3.2 edastatud kõigile mõjutatud meeskondadele ja kajastatud ajakohastatud teadlikkuse tõstmise koolituses;

9.3.3 valideeritud lauaõppuste või praktiliste intsidentidele reageerimise õppuste kaudu kolme kuu jooksul pärast heakskiitmist.

9.4 Kiireloomulised ajakohastused, mis on tingitud esilekerkivatest ohtudest, auditileidudest või uutest õiguslikest kohustustest, tuleb rakendada viivitamata ja märkida poliitika versiooniajaloos.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat toetavad ja sellega on seotud järgmised organisatsiooni poliitikad:

10.1.1 P1 – infoturbepoliitika: kehtestab üldise nõude riskipõhiseks ja intsidentideks valmis tegevuskorralduseks.

10.1.2 P5 – muudatuste haldamise poliitika: tagab, et taristu või teenustega seotud ohjeldamise ja taastamise tegevused järgivad ametlikke protseduure.

10.1.3 P13 – andmete klassifitseerimise ja märgistamise poliitika: toetab intsidendi raskusastme klassifitseerimist andmete tundlikkuse alusel.

10.1.4 P15 – varundamise ja taastamise poliitika: võimaldab lunavara või hävitavate rünnakute järel taastamist koos tervikluse tagamisega.

10.1.5 P18 – krüptograafiliste kontrollimeetmete poliitika: määratleb krüptimismeetmed, mis vähendavad intsidendi mõju ja andmete avalikuks saamise riski.

10.1.6 P22 – logimise ja seire poliitika: loob tõhusaks tuvastamiseks ja kohtuekspertiisiks vajaliku alusnähtavuse sündmustele, teavitustele ja logide säilitamisele.

10.1.7 P29 – testandmete ja testkeskkondade poliitika: tagab, et ka tootmisväliseid süsteeme mõjutavaid intsidente käsitletakse struktureeritud ja turvalisel viisil.

10.1.8 P33 – auditi ja vastavusseire poliitika: valideerib intsidentideks valmisolekut ja reageerimise tõhusust struktureeritud auditite ning vastavushindamiste kaudu.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001: punkt 8.1 – tegevuste kavandamine ja kontroll: struktureeritud protsessid riskide juhtimiseks ja intsidentidele reageerimise kavandamiseks.

11.2 ISO/IEC 27002:2022 – kontrollimeetmed 5.25–5.27: vastutus intsidendihalduse, intsidentidest teatamise, reageerimise, teabevahetuse ja täiustamise eest.

11.3 NIST SP 800-53 Rev.5: IR-1 kuni IR-9, AU-6, PL-2: terviklikud nõuded intsidentidele reageerimise elutsüklile, auditile ja turbeplaneerimisele.

11.4 EL GDPR: artikkel 33/34: järelevalveasutustele teatamise kohustused ja andmesubjektide teavitamise nõuded (koos määratletud eranditega).

11.5 EL NIS2 direktiiv (2022/2555): artikkel 23: kohustuslik riiklik aruandlus, sealhulgas vahearuandluse ja lõpparuandluse nõuded.

11.6 EL DORA (2022/2554): artikkel 17: finantsasutuste IKT-intsidentidest pädevatele asutustele teatamise nõuded.

11.7 COBIT 2019: DSS02, DSS04, MEA01: teenuseintsidentide ja talitluspidevuse juhtimine ning toimivuse ja vastavuse seire.