					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P30S					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	Punktid 6.1, 6.3, 8	Intsidentide haldus, pidev täiustamine, operatiivjuhtimine
ISO/IEC 27002:2022	Kontrollimeetmed 5.24, 5.25	Intsidentide tuvastamine, valmisolek, õppimine
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Intsidentide käsitlemine, seire ja teavitamine
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 33	Rikkumisest teavitamise nõuded
ELi NIS2 direktiiv	Artikkel 23	Kohustuslik küberintsidentidest teatamine
ELi DORA määrus	Artikkel 17	IKT-intsidentide haldus
COBIT 2019	DSS02, DSS04	Teenusetaotluste ja intsidentide haldus ning talitluspidevus

1. Eesmärk

1.1. Käesolev poliitika sätestab, kuidas organisatsioon tuvastab, registreerib, teatab ja lahendab infoturbeintsidente, mis mõjutavad organisatsiooni digitaalseid süsteeme, andmeid või teenuseid.

1.2. Poliitika eesmärk on võimaldada organisatsioonil minimeerida kahju, kaitsta kliendiandmeid ja täita regulatiivseid kohustusi, sealhulgas GDPR-ist tulenevat 72-tunnist rikkumisest teatamise nõuet.

1.3. Poliitika tagab selged vastutused, teabevahetuse sammud ja intsidendijärgsed tegevused ka väikestes organisatsioonides, kus puudub eraldi infoturbemeeskond.

2. Kohaldamisala

2.1. Käesolev poliitika kohaldub järgmisele:

2.1.1. kõik töötajad, töövõtjad ja välised IT-teenuse osutajad;

2.1.2. kõik organisatsiooni hallatavad süsteemid ja teenused, sealhulgas veebilehed, pilveplatvormid, mobiiltelefonid, sülearvutid ja e-posti kontod;

2.1.3. kõik intsidendiliigid, sealhulgas:

2.1.3.1. loata juurdepääs andmetele või süsteemidele;

2.1.3.2. pahavaranakkused või lunavara;

2.1.3.3. andmepüügikatsed või sotsiaalne manipulatsioon;

2.1.3.4. küberrünnakust või väärkasutusest tingitud süsteemikatkestused;

2.1.3.5. tundliku teabe juhuslik avalikustamine või kustutamine;

2.1.3.6. äriseadmete või teisaldatavate andmekandjate kaotus või vargus.

3. Eesmärgid

3.1. Kehtestada selge protsess turbeintsidentide tuvastamiseks ja eskaleerimiseks.

3.2. Tagada, et intsidentidest teatatakse, need registreeritakse ning nende suhtes rakendatakse meetmeid eelnevalt kindlaksmääratud tähtaegade jooksul.

3.3. Võimaldada kahju kiire ohjeldamine ning andmete ja teenuste taastamine.

3.4. Tagada, et mõjutatud osapooli (nt kliendid, regulaatorid) teavitatakse, kui see on õigusaktidest tulenevalt nõutav.

3.5. Vältida kordumist algpõhjuse analüüsi, parandusmeetmete ja poliitika täiustamise kaudu.

3.6. Võimaldada VKE-del täita ISO/IEC 27001 sertifitseerimisnõudeid ja tõendada auditite käigus vastutust.

4. Rollid ja vastutused

4.1. Tegevjuht (GM)

4.1.1. Vastutab käesoleva poliitika eest ja tagab selle rakendamise.

4.1.2. Teostab järelevalvet intsidentidele reageerimise tegevuste üle ning kiidab heaks regulaatoritele või klientidele edastatavad teavitused.

4.1.3. Vaatab läbi intsidendijärgsed aruanded ja tagab poliitika ajakohastamise vajaduse korral.

4.1.4. Võib delegeerida koordineerimisülesandeid, kuid säilitab vastutuse.

4.2. IT-teenuse osutaja / süsteemiadministraator (sisemine või väline)

4.2.1. Tuvastab ja uurib võimalikke turbeintsidente.

4.2.2. Rakendab ohjeldus- ja taastemeetmeid (nt juurdepääsu keelamine, varukoopiatest taastamine).

4.2.3. Teavitab tegevjuhti kõigist kinnitatud või kahtlustatavatest intsidentidest ühe tunni jooksul alates nende avastamisest.

4.2.4. Peab intsidentide logi, mis sisaldab ajatemplid, mõjuhinnangut ja reageerimistegevusi.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Korrapärane läbivaatamine

9.1.1. Tegevjuht (GM) peab käesoleva poliitika läbi vaatama vähemalt üks kord iga 12 kuu järel, et tagada:

9.1.1.1. kooskõla ISO/IEC 27001:2022 kontrollimeetmetega;

9.1.1.2. reageerimisvõime uutele ohtudele, riskidele ja intsidentidele;

9.1.1.3. jätkuv vastavus õiguslikele ja lepingulistele kohustustele (nt GDPR, DORA).

9.2. Läbivaatamise aluseks olevad sündmused

9.2.1. Poliitika tuleb läbi vaadata ja ajakohastada ka pärast järgmist:

9.2.1.1. mis tahes kõrge tõsidusega intsident või regulatiivne teavitus;

9.2.1.2. uue IT-taristu kasutuselevõtt või süsteemimuudatused;

9.2.1.3. turberikkumisi käsitlevate õigusnõuete muudatused.

9.3. Läbivaatamise dokumenteerimine ja levitamine

9.3.1. Kõik läbivaatamised ja muudatused tuleb dokumenteerida poliitika muudatuste logis.

9.3.2. Ajakohastatud versioonid tuleb edastada kõigile töötajatele, tarnijatele ja IT-teenuse osutajatele, kes on seotud infoturbe või süsteemide käitamisega.

9.3.3. Auditivalmiduse tagamiseks tuleb säilitada tõendid töötajate teadlikkuse kohta (nt koosolekumärkmed või e-posti kinnitused).

10. Seotud poliitikad ja seosed

10.1. Käesolevat poliitikat tuleb rakendada kooskõlas järgmiste VKE poliitikatega:

10.1.1. P1S – Infoturbepoliitika: määratleb üldised ootused konfidentsiaalsuse, tervikluse ja käideldavuse säilitamiseks tegevuste käigus, sealhulgas intsidentide käsitlemisel.

10.1.2. P2S – Juhtimisrollide ja vastutuste poliitika: kehtestab volituste ja vastutuse struktuuri intsidendi tuvastamiseks, sellest teatamiseks ja eskaleerimiseks.

10.1.3. P4S – Juurdepääsukontrolli poliitika: võimaldab intsidentidele reageerimise käigus juurdepääsuõiguste viivitamatut tühistamist.

10.1.4. P8S – Infoturbeteadlikkuse koolituse poliitika: tagab, et kõik töötajad suudavad turbeintsidente tõhusalt tuvastada ja neist teatada.

10.1.5. P17S – Andmekaitse ja privaatsuspoliitika: suunab GDPR-ist tulenevaid rikkumisest teatamise õiguslikke protseduure ning toetab õigusnormidele vastavust intsidentide ajal.

10.1.6. P22S – Logimise ja seire poliitika: annab turbesündmuste tuvastamiseks, analüüsimiseks ja auditeerimiseks vajalikud vahendid ja nähtavuse.

10.1.7. P31S – Tõendite kogumise ja kohtueksperti poliitika: toetab intsidendiga seotud tegevuste uurimist ja õiguslikku kaitstavust, suunates tõendite nõuetekohast käitlemist.

10.2. Need poliitikad moodustavad koos VKE operatiivse raamistiku infoturbeintsidentide tuvastamiseks, neile reageerimiseks ja neist taastumiseks.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 6.1 – nõuab riskikäsitluse planeerimist, sealhulgas intsidentideks valmistumist.

11.1.2. Punkt 6.3 – toetab pidevat täiustamist turbesündmustest saadud õppetundide kaudu.

11.1.3. Punkt 8.1 – rõhutab operatiivjuhtimist intsidentide ja häirete haldamisel.

11.2. ISO/IEC 27002

11.2.1. Kontroll 5.24 – nõuab struktureeritud lähenemist infoturbeintsidentidest teatamiseks, nende hindamiseks ja neile reageerimiseks.

11.2.2. Kontroll 5.25 – keskendub intsidentidest õppimisele, et parandada tulevast valmisolekut ja süsteemide toimepidevust.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – määratleb intsidendikäitluse protseduurid, sealhulgas ohjeldamise ja taastamise.

11.3.2. IR-5 – kehtestab intsidendiseire ja -analüüsi nõuded.

11.3.3. IR-6 – nõuab sisemisi ja väliseid intsidentidest teatamise protseduure.

11.4. ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1. Artikkel 33 – nõuab isikuandmete rikkumistest teatamist regulaatoritele 72 tunni jooksul koos ulatuse ja maandamismeetmete üksikasjadega.

11.5. ELi NIS2 direktiiv (2022/2555)

11.5.1. Artikkel 23 – nõuab olulistelt ja tähtsatelt üksustelt olulistest intsidentidest teatamist pädevatele asutustele standarditud teavitusvormingute abil.

11.6. ELi DORA määrus (2022/2554)

11.6.1. Artikkel 17 – nõuab finantsüksustelt IKT-ga seotud intsidentide ja häirete liigitamist, neist teatamist ning nende jälgimist.

11.7. COBIT 2019

11.7.1. DSS02 – Teenusetaotluste ja intsidentide haldamine: suunab operatiivsete ja turbeintsidentide tõhusat käsitlemist kooskõlas juhtimiseesmärkidega.

11.7.2. DSS04 – Talitluspidevuse haldamine: seob intsidentidele reageerimise laiemate talitluspidevuse ja taaste strateegiatega.