					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P13					Dokumendi pealkiri: **Andmete klassifitseerimise ja märgistamise 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**

1. Eesmärk

1.1 Käesolev poliitika määratleb ametliku raamistiku organisatsiooni teabevarade klassifitseerimiseks ja märgistamiseks nende tundlikkuse, riskipositsiooni ja regulatiivsete kohustuste alusel.

1.2 Sellega tagatakse, et kogu teave, olenemata sellest, kas seda säilitatakse, edastatakse või töödeldakse, on selgelt kategoriseeritud ja märgistatud viisil, mis väljendab nõutavat kaitse- ja käitlustaset.

1.3 Käesolev poliitika nõuab struktureeritud klassifitseerimist kooskõlas organisatsiooni riskijuhtimise tavadega, toetades konfidentsiaalsuse, tervikluse ja käideldavuse eesmärke nii digitaalsete kui ka füüsiliste andmeliikide puhul.

1.4 See kontrollimeede on oluline rollipõhise juurdepääsu, auditivalmiduse, asjakohase andmejagamise ning selliste tehniliste kaitsemeetmete nagu krüptograafia, varundamine ja seire tõhusaks rakendamiseks.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmise suhtes:

2.1.1 kõik organisatsiooni teabevarad, sealhulgas dokumendid, andmebaasid, kirjed ja side

2.1.2 kõik andmevormingud, sealhulgas digitaalsed, trükitud, kirjalikud ja suulised

2.1.3 kõik keskkonnad: kohapealsed, kaug-, mobiilsed ja pilvekeskkonnad

2.1.4 kõik töötajad, töövõtjad, teenuseosutajad ja kolmandad osapooled, kes loovad, käitlevad või säilitavad organisatsiooni teavet

2.2 Kohaldamisala hõlmab organisatsioonisiseselt loodud sisu, välistest allikatest saadud andmeid, andmekaitsealaste õigusaktide kohaldamisalasse kuuluvaid isikuandmeid (nt GDPR) ning klientide, partnerite ja regulaatoritega vahetatavat teavet.

2.3 See kehtib kõigi andmete säilitamiseks või edastamiseks kasutatavate süsteemide suhtes, sealhulgas ettevõtterakendused, failiserverid, e-posti süsteemid, pilveplatvormid ja varukoopiate hoidlad.

3. Eesmärgid

3.1 Kehtestada standardne, kogu organisatsiooni hõlmav klassifitseerimisskeem, mis põhineb andmete avalikustamise või kompromiteerimise mõjul.

3.2 Tagada, et kogu teave on nähtavalt ja püsivalt märgistatud viisil, mis kajastab selle klassifitseerimistaset ja käitlusnõudeid.

3.3 Rakendada andmekäitluse ja juurdepääsukontrolli kontrollimeetmeid kooskõlas klassifitseerimisega, sealhulgas krüptograafiat, logimist, edastuse kaitset ja säilitustähtaegu.

3.4 Toetada vastavust rahvusvahelistele standarditele (ISO/IEC 27001, 27002), õigusraamistikele (GDPR, NIS2, DORA) ja organisatsiooni sisemistele riskipoliitikatele.

3.5 Tagada, et kõik kasutajad mõistavad oma vastutust andmete kaitsmisel, märgiste rakendamisel ja klassifitseeritud teabe nõuetekohasel käitlemisel.

3.6 Säilitada jälgitavus klassifitseerimisstaatuse, seotud kontrollimeetmete ja organisatsiooni vararegistri vahel auditi ja nõuetele vastavuse eesmärgil.

4. Rollid ja vastutused

4.1 infoturbe juht (CISO)

4.1.1 Vastutab teabe klassifitseerimise ja märgistamise poliitika eest ning tagab selle vastavuse regulatiivsetele, lepingulistele ja tegevusnõuetele.

4.1.2 Kinnitab klassifitseerimistasemed, märgistamisstandardid ja poliitika muudatused.

4.1.3 Teostab järelevalvet poliitika järgimise üle auditite, mõõdikute ja erandite läbivaatamise kaudu.

4.1.4 Koordineerib tegevusi õigus- ja vastavusfunktsiooni, andmekaitse ja riskijuhtimisega.

4.2 teabevara omanikud

4.2.1 Vastutavad oma kontrolli all olevate teabevarade klassifitseerimise eest, kasutades organisatsiooni klassifitseerimisskeemi.

4.2.2 Rakendavad klassifitseerimismärgiseid teabe loomisel, ajakohastamisel või vastuvõtmisel.

4.2.3 Vaatavad varade klassifikatsiooni perioodiliselt üle, eelkõige tundlikkuse, regulatiivse kohaldamisala või äriväärtuse muutumisel.

4.2.4 Tagavad, et tundlikke andmeid käideldakse ja märgistatakse asjakohaselt kogu nende elutsükli vältel.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata, et tagada kooskõla järgmisega:

9.1.1 muutuvad regulatiivsed nõuded (nt GDPR, NIS2, DORA)

9.1.2 ISO/IEC 27001 või 27002 klassifitseerimisjuhiste uuendused

9.1.3 organisatsioonilised muudatused, mis mõjutavad andmete tundlikkust või vastutust

9.1.4 tehnoloogilised muudatused, sealhulgas uued dokumendi- või andmehaldusplatvormid

9.2 infoturbe juht (CISO) peab algatama läbivaatamise koostöös infoturbe komitee, õigusnõustaja ja mõjutatud äriüksustega.

9.3 Läbivaatamised peavad hõlmama järgmist:

9.3.1 klassifitseerimise jõustamise tõhusus ja kasutajate poliitika järgimine

9.3.2 valeklassifitseerimisega seotud intsidentide või erandite analüüs

9.3.3 kasutajate tagasiside märgistamistööriistade või juhendmaterjalide kohta

9.3.4 võrdlus valdkonna klassifitseerimisstandarditega

9.4 Poliitikauuendused peavad olema versioonihalduses, dokumenteeritud ISMS-i hoidlas ning edastatud kõigile asjaomastele töötajatele, rõhutades uusi vastutusi või tööriistamuudatusi.

9.5 Uusi töötajaid tuleb tööle asumisel tutvustada poliitika kehtiva versiooniga. Kõik töötajad peavad pärast olulisi poliitikamuudatusi läbima korduskoolituse.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat toetavad vahetult ja selles kirjeldatud kontrollimeetmeid rakendavad järgmised seotud poliitikad:

10.1.1 P4 - Juurdepääsukontrolli poliitika: juurdepääsu teabele juhitakse klassifitseerimistasemete alusel; tundlikumad andmed nõuavad rangemat juurdepääsukontrolli ja autoriseerimismehhanisme.

10.1.2 P11 - Kasutajakontode ja õiguste haldamise poliitika: tugevdab õiguste määramist teadmisvajaduse alusel, lähtudes klassifitseerimistasemetest.

10.1.3 P12 - Varahalduse poliitika: tagab, et vararegistris on iga vara juures selle klassifikatsioon ja märgis, toetades jälgitavust ja vastutust.

10.1.4 P14 - Andmete säilitamise ja kõrvaldamise poliitika: kõrvaldamise ja säilitamise reeglid määratakse andmete klassifitseerimistaseme ning regulatiivsete säilitamisnõuete alusel.

10.1.5 P18 - Krüptograafiliste kontrollimeetmete poliitika: rakendab asjakohaseid krüptograafiastandardeid teabevara klassifikatsiooni alusel.

10.1.6 P22 - Logimise ja seire poliitika: võimaldab seirata juurdepääsu klassifitseeritud teabele ja selle liikumist, tagades auditivalmiduse ning valemärgistamise või väärkasutuse tuvastamise.

10.2 Iga seos tagab teabe järjepideva kaitse kogu selle elutsükli vältel alates loomisest ja klassifitseerimisest kuni turvalise käitlemise, säilitamise, edastamise ja lõpliku hävitamiseni.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud standardite ja regulatiivsete raamistikega, mis reguleerivad tundliku teabe klassifitseerimist ja märgistamist.

11.2 ISO/IEC 27001

11.2.1 Punkt 4.2 - huvitatud osapoolte vajaduste ja ootuste mõistmine. Klassifitseerimisnõuded tulenevad sageli huvitatud osapoolte kehtestatud õiguslikest, regulatiivsetest või lepingulistest kohustustest (nt GDPR, kliendi konfidentsiaalsuslepingud (NDA)), mis peavad poliitikas kajastuma.

11.2.2 Punkt 6.1.3 - infoturbe riskikäsitlus. Klassifitseerimine mõjutab otseselt riskikäsitluse kontrollimeetmete valikut, sealhulgas juurdepääsukontrolli, krüptograafiat ja säilitamist, lähtudes andmete tundlikkusest.

11.2.3 Punkt 7.2 - pädevus. Käesolev poliitika nõuab, et klassifitseerimise ja märgistamise eest vastutav personal oleks koolitatud, mis kuulub pädevusnõuete alla.

11.2.4 Punkt 7.3 - teadlikkus. Käesolev poliitika nõuab, et kõik kasutajad oleksid teadlikud klassifitseerimistasemetest ja oma vastutusest teabe käitlemisel, olles kooskõlas teadlikkuse nõuetega.

11.2.5 Punkt 7.5 - dokumenteeritud teave. Klassifitseerimispoliitika ise on kontrollitud dokument ning protseduurid, koolituskirjed ja klassifitseerimismärgised kuuluvad dokumenteeritud teabe hulka.

11.2.6 Punkt 8.1 - operatiivne planeerimine ja kontroll. Klassifitseerimine ja märgistamine on operatiivsed protsessid, mis on lõimitud andmete elutsükli haldusesse, ning see punkt tagab, et sellised tegevused on planeeritud, rakendatud ja kontrollitud.

11.2.7 Punkt 9.1 - seire, mõõtmine, analüüs ja hindamine. Käesolev poliitika sisaldab sätteid klassifitseerimise vastavuse, intsidenditrendide ja märgistamisskeemi tõhususe seireks.

11.2.8 Punkt 10.1 - mittevastavus ja parandusmeetmed. Käesolev poliitika määratleb reageerimise valeklassifitseerimisele, sealhulgas parandusmeetmed nagu ümberõpe, ajakohastused ja erandite käsitlemine.

11.3 ISO/IEC 27002:2022

11.3.1 Kontroll 5.12 - teabe klassifitseerimine. See kontrollimeede tagab, et teave klassifitseeritakse selle tundlikkuse, väärtuse ja kriitilisuse alusel - täpselt seda käesolev poliitika formaliseerib.

11.3.2 Kontroll 5.13 - teabe märgistamine. See kontrollimeede nõuab teabe asjakohast märgistamist vastavalt selle klassifitseerimistasemele, mida käesolev poliitika käsitleb täielikult.

11.3.3 Kontroll 5.10 - teabe ja muude seotud varade lubatud kasutus. Käesolev poliitika sätestab, kuidas kasutajad peavad klassifitseeritud andmeid käitlema, toetades otseselt lubatud kasutuse põhimõtteid ja ennetades väärkasutust.

11.3.4 Kontroll 5.11 - varade tagastamine. Klassifitseerimine aitab tagada, et tundlikud andmed on tuvastatud ning töötaja või tarnija lahkumisel turvaliselt tagastatud või puhastatud.

11.3.5 Kontroll 5.9 - teabe ja muude seotud varade register. Klassifitseerimine on sageli seotud varade registriga, mis peab iga kirje puhul kajastama klassifitseerimistaset, et toetada kontrollimeetmete asjakohast määramist.

11.3.6 Kontroll 5.14 - teabe edastamine. Klassifitseerimistasemed mõjutavad organisatsioonisiseste ja väliste andmeedastuste kontrollimeetmeid (nt krüptograafia, heakskiit, juurdepääsupiirangud).

11.3.7 Kontroll 8.12 - andmelekke vältimine. Klassifitseerimise ja märgistamise rakendamine toetab loata avalikustamise ja andmekao vältimist.

11.3.8 Kontroll 8.11 - andmete maskeerimine. Teatud klassifitseerimistasemed (nt Konfidentsiaalne, Piiratud) võivad nõuda maskeerimist, kui andmeid kasutatakse testimis- või arenduskeskkonnas või analüütikas.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-2 - süsteemi ja side kaitse poliitika ning protseduurid: toetab klassifitseerimispoliitikaid kui osa üldisest andmekaitsest.

11.4.2 AC-16 - turbeatribuudid: rakendab juurdepääsu jõustamist klassifitseerimise metaandmete ja kasutajate juurdepääsuõiguste alusel.

11.4.3 MP-3 / MP-5 - andmekandjate märgistamine ja transpordikaitse: jõustab andmete märgistamise ja kaitse nii säilitamisel kui ka edastamisel klassifitseerimise alusel.

11.5 EL GDPR (2016/679)

11.5.1 Artikkel 5 - andmekaitse põhimõtted: nõuab, et isikuandmeid töödeldaks turvaliselt ja proportsionaalselt nende tundlikkusega.

11.5.2 Artikkel 32 - töötlemise turvalisus: tugevdab klassifitseerimist kui riskipõhise andmekaitse ja asjakohaste tehniliste ning korralduslike meetmete mehhanismi.

11.6 EL NIS2 direktiiv (2022/2555)

11.6.1 Artikkel 21(2)(a): nõuab infoturbe riskijuhtimise poliitikaid, sealhulgas varade ja andmete klassifitseerimise kontrollimeetmeid.

11.6.2 Artikkel 21(3): soodustab sobivate andmekäitlusmeetmete rakendamist - seda toetab klassifitseerimisel põhinev märgistamine.

11.7 EL DORA (2022/2554)

11.7.1 Artikkel 5 - juhtimine ja kontroll. Nõuab juhtimisraamistikke, mis klassifitseerivad andmevarasid IKT-riski kontrollimiseks.

11.7.2 Artikkel 9 - IKT-riskide juhtimine. Kehtestab tehnilised ja korralduslikud meetmed kriitilistele IKT-varadele, sealhulgas klassifitseerimise ja märgistamise.

11.8 COBIT 2019

11.8.1 DSS05.02 - turbeteenuste haldamine: jõustab infoturbe klassifitseerimise, et tagada ettevõtte andmete kaitse.

11.8.2 MEA03 - vastavuse seire, hindamine ja auditeerimine: toetab klassifitseerimistavade regulaarset auditit ja läbivaatamist, et tagada poliitika järgimine ja küpsus.