					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P13S					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**

Vastavus standarditele ja õigusaktidele

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.3, 8	
ISO/IEC 27002:2022	Kontrollid 5.12, 5.13	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
EL NIS2	Artikkel 21(2)(a)	
EL DORA	Artikkel 5(8)	
COBIT 2019	BAI03.05, DSS05	
EL GDPR	Artikkel 5, 32	

1. Eesmärk

1.1 Käesolev poliitika määratleb, kuidas kogu organisatsiooni hallatav teave tuleb klassifitseerida ja märgistada, et tagada selle konfidentsiaalsus, terviklus ja käideldavus kogu elutsükli jooksul.

1.2 Poliitika toetab ühtset andmekäitlust, määrates teabele asjakohase kaitsetaseme vastavalt selle tundlikkusele, ärimõjule või õiguslikele kohustustele.

1.3 Klassifitseerimine ja märgistamine aitavad vähendada tundlike andmete juhusliku avaldamise, loata juurdepääsu või väärkäitluse riski, eriti VKE-des, mis võivad tugineda lihtsamatele süsteemidele ja vähem formaliseeritud kontrollimeetmetele.

1.4 Käesolev poliitika on oluline ISO/IEC 27001 sertifitseerimise ja õigusnõuetele vastavuse tagamise seisukohast, eelkõige andmekaitsenõuete, nagu GDPR, ning küberturberaamistike, nagu NIS2 ja DORA, kontekstis.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile organisatsiooni andmetele sõltumata nende vormist või asukohast, sealhulgas:

2.1.1 elektroonilised dokumendid, tabelid, e-kirjad, vormid, pildid ja skannitud failid;

2.1.2 füüsilised dokumendid, nagu väljatrükitud kirjed, aruanded, arved ja märkmed;

2.1.3 andmed, mida säilitatakse või töödeldakse pilveteenustes, kohalikes serverites, eemaldatavatel andmekandjatel või äritegevuses kasutatavates isiklikes seadmetes;

2.1.4 ajutised või üleminekuandmed, mis tekivad äritegevuse käigus (nt logid, vahemälufailid, e-kirjad).

2.2 Kõik töötajad, töövõtjad, ajutised töötajad ja välised teenuseosutajad, kellel on juurdepääs organisatsiooni andmetele, peavad käesolevat poliitikat järgima.

2.3 Poliitika kehtib kogu andmete elutsükli jooksul alates loomisest ja säilitamisest kuni juurdepääsu, edastamise, arhiveerimise või kustutamiseni.

3. Eesmärgid

3.1 Määratleda lihtne ja rakendatav klassifitseerimisskeem, mida on kogu organisatsioonis lihtne mõista ja kasutada.

3.2 Nõuda, et iga andmevara klassifitseeritakse vastavalt selle tundlikkusele ja märgistatakse sellele vastavalt, et suunata nõuetekohast käitlemist, säilitamist ja juurdepääsu.

3.3 Tagada, et andmete märgistamise tavad on lõimitud äriprotsessidesse, nagu tööle asumine, projekti käivitamine ja süsteemide seadistamine.

3.4 Vähendada andmekaitserikkumise riski, rakendades käitlemise kontrollimeetmeid (nt krüpteerimine, juurdepääsupiirangud) vastavalt klassifikatsioonitasemele.

3.5 Tagada vastavus andmekaitse- ja infoturbenõuetele, tõendades, et tundlikud andmed (nt isikuandmed, finantsandmed või ärisaladused) on nõuetekohaselt märgistatud ja hallatud.

3.6 Kehtestada vastutus klassifitseerimisotsuste eest ning tagada nende perioodiline läbivaatamine ja ajakohastamine vastavalt muutuvatele äri- ja õiguslikele vajadustele.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Vastutab käesoleva poliitika eest ja kiidab heaks klassifitseerimisskeemi.

4.1.2 Tagab järelevalve selle üle, et klassifitseerimisega seotud vastutused on delegeeritud ja rakendatud.

4.1.3 Vaatab läbi ja kiidab heaks kõik erandid klassifitseerimise või märgistamise nõuetest.

4.1.4 Tagab, et andmekäitlustavad vastavad GDPR-i, DORA ja teiste asjakohaste õigusaktide nõuetele.

4.2 Teabe omanik / andmehaldur

4.2.1 Määrab igale uuele andmekogumile või teabevarale esialgse klassifikatsiooni selle loomisel või omandamisel.

4.2.2 Tagab, et nähtavad märgised (nt faili päised, jalused, vesimärgid, kaustanimed) rakendatakse seal, kus see on asjakohane.

4.2.3 Vaatab klassifikatsioonid perioodiliselt üle, et hinnata nende asjakohasust, täpsust ja vajalikke muudatusi (nt pärast salastatuse lõpetamist või avaldamist).

4.2.4 Teeb koostööd IT-juhiga, et rakendada klassifikatsioonist tulenevaid tehnilisi kaitsemeetmeid (nt juurdepääsuõigused, krüpteerimine).

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb tegevjuhi ja andmehalduri poolt kord aastas läbi vaadata, et tagada selle vastavus järgmistele muudatustele:

9.1.1 muudatused äritegevuses või andmeliikides;

9.1.2 uued regulatiivsed nõuded (nt andmekaitse või finantsjärelevalve);

9.1.3 tehnoloogilised muudatused, mis mõjutavad märgistamise või klassifitseerimise võimekust.

9.2 Läbivaatamine peab hõlmama klassifitseerimiskategooriate, märgistamisvahendite või -tavade ning teadlikkuse suurendamise ja koolituse sisu ajakohastamist.

9.3 Poliitikamuudatused peab heaks kiitma tegevjuht ning need tuleb teatavaks teha kõigile töötajatele. Auditi eesmärgil tuleb säilitada kirje versioonimuudatuste kohta.

10. Seotud poliitikad ja seosed

10.1 P2S – Juhtimisrollide ja vastutuste poliitika: määrab vastutuse poliitika omamise ja rakendamise eest.

10.2 P4S – Juurdepääsukontrolli poliitika: seob süsteemidele antava juurdepääsu andmete klassifikatsioonitasemetega.

10.3 P12S – Varahalduse poliitika: hõlmab füüsilisi ja digitaalseid varasid, milles säilitatakse klassifitseeritud andmeid.

10.4 P17S – Andmekaitse ja privaatsuse poliitika: reguleerib isikuandmete kaitset, millest suur osa on klassifitseeritud kui Konfidentsiaalne.

10.5 P30S – Intsidentidele reageerimise poliitika: määratleb eskaleerimisteed ja reageerimisprotseduurid klassifitseerimisrikkumiste või andmete avalikustumise korral.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 5.3: nõuab selgelt määratletud vastutusi andmete käitlemisel ja kaitsmisel.

11.1.2 Punkt 8.1: nõuab tegevuslikku planeerimist ja kontrollimeetmeid, sealhulgas andmete kategoriseerimisega seotud meetmeid.

11.2 ISO/IEC 27002

11.2.1 Kontroll 5.12: annab suunised teabe klassifitseerimiseks riski ja regulatiivsete nõuete alusel.

11.2.2 Kontroll 5.13: kirjeldab praktilisi märgistamismehhanisme ja nendega seotud käitlemisreegleid.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: nõuab teabe märgistamist, et kaitsemeetmed oleksid kooskõlas klassifikatsiooniga.

11.3.2 MP-3 / MP-5: annavad suuniseid andmekandjate ja väljundite märgistamiseks ning kontrollimiseks.

11.4 EL GDPR

11.4.1 Artikkel 5 ja 32: nõuavad andmete minimaalsuse ja tervikluse tagamist asjakohaste klassifitseerimis- ja käitlemiskaitsemeetmete kaudu.

11.5 EL NIS2

11.5.1 Artikkel 21(2)(a): nõuab riskipõhiseid tehnilisi ja korralduslikke meetmeid andmete kaitseks.

11.6 EL DORA

11.6.1 Artikkel 5(8): nõuab, et ettevõtted klassifitseeriksid andmevarad IKT-riskide juhtimise programmi osana.

11.7 COBIT 2019

11.7.1 BAI03.05: nõuab teabe klassifitseerimist ja riskipõhist kaitset.

11.7.2 DSS05.02: käsitleb klassifikatsioonipõhiste kontrollimeetmete rakendamist ja seiret.