					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P25S					Dokumendi pealkiri: **Rakenduste turbenõuete 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	Operatiivsed kontrollimeetmed, sealhulgas rakenduste turve
ISO/IEC 27002:2022	Kontrollid 8.25–8.26	Turvaline kavandamine, arendamine, testimine ja koodi läbivaatus
NIST SP 800-53 Rev.5	SA-11, SI-10	Arendaja- ja rakendustestimine, koodianalüüs, puuduste ennetamine
EL GDPR	Artikkel 25	Andmekaitse kavandamisel ja vaikimisi andmekaitse
EL NIS2	Artikkel 21(2)(a), (e)	Tehnilised meetmed rakenduste kaitsmiseks ja riskide tuvastamiseks
EL DORA	Artikkel 9(2)(c), 10(2)(c)	Rakenduste turve digitaalse operatiivse toimepidevuse tagamiseks
COBIT 2019	BAI03	Turvalise tarkvara arendamise või hankimise juhtimine

1. Eesmärk

1.1 Käesolev poliitika määratleb minimaalsed kohustuslikud rakenduste turbe kontrollimeetmed, mida nõutakse kõigi organisatsioonis kasutatavate tarkvara- ja süsteemilahenduste puhul, sõltumata sellest, kas need on arendatud ettevõttesiseselt või hangitud välistelt tarnijatelt.

1.2 See tagab, et rakendused kavandatakse, rakendatakse ja hallatakse viisil, mis kaitseb klientide, töötajate ja ettevõtte andmeid loata juurdepääsu, väärkasutuse, muutmise või hävitamise eest.

1.3 Käesolev poliitika toetab organisatsiooni ISO/IEC 27001 sertifitseerimise saavutamisel ja säilitamisel, GDPR-i ja NIS2 kohustuste täitmisel ning ebaturvalise tarkvara juurutamisega seotud tegevusriskide vähendamisel.

1.4 See aitab luua VKEdele ühtse ja auditikõlbliku lähenemise rakenduste turbele, kehtestades ühtse turvafunktsioonide ja praktikate kontrollnimekirja, mis on kohandatud keskkondadele, kus ettevõttesisesed tehnilised ressursid on piiratud.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile rakendustele, süsteemidele, tööriistadele ja platvormidele, mis:

2.1.1 on arendatud ettevõttesiseselt, kohandatud või skriptitud sisekasutuseks;

2.1.2 on hangitud kommertstarkvarana, SaaS-lahendusena või pilvekeskkonnas kasutatavate süsteemidena;

2.1.3 töötlevad, salvestavad või edastavad isikuandmeid, tegevuskirjeid või tundlikku operatiivteavet;

2.1.4 on töötajatele, töövõtjatele, klientidele või partneritele kättesaadavad sisevõrkude, interneti või mobiiliplatvormide kaudu.

2.2 Poliitika hõlmab:

2.2.1 arendajaid (sisemisi või lepingulisi);

2.2.2 tarkvaratarnijaid ja pilveteenuse pakkujaid;

2.2.3 IT-toe personali või administraatoreid, kes vastutavad juurutamise ja toe eest;

2.2.4 rakenduste omanikke ja ärikasutajaid, kes osalevad süsteemide heakskiitmises ja järelevalves.

3. Eesmärgid

3.1 Tagada, et kõigil organisatsioonis kasutatavatel rakendustel on integreeritud ja kontrollitavad turbekontrollid, mis maandavad levinud tarkvarahaavatavusi.

3.2 Kaitsta rakenduste töödeldavate andmete konfidentsiaalsust, terviklust ja käideldavust sõltumata nende majutuskohast.

3.3 Nõuda rakenduste turbe ametlikku testimist, ülevaatust ja valideerimist enne uue rakenduse või olulise uuenduse heakskiitmist tootmiskasutuseks.

3.4 Tagada kasutajate autentimisandmete, seansiandmete ja juurdepääsuõiguste ühtne ning turvaline käitlemine kõigis ärikriitilistes süsteemides.

3.5 Nõuda kõigis rakendustes turvalisi logimis-, auditeerimis- ja seirefunktsioone, et toetada kahtlase tegevuse tuvastamist ja sellele reageerimist.

3.6 Vähendada õigus- ja vastavusriske, tagades, et rakendused vastavad kohaldatavatele regulatiivsetele turbenõuetele.

4. Rollid ja vastutused

4.1 Tegevjuht

4.1.1 Vastutab üldiselt rakenduste turbe eest kogu organisatsioonis.

4.1.2 Kiidab heaks käesoleva poliitika ning tagab, et kõik hanke- ja arendusprojektid järgivad seda.

4.1.3 Tagab, et tarnijatele ja teenuseosutajatele on lepinguliselt kehtestatud rakenduste turbenõuded.

4.1.4 Vaatab läbi ja kiidab heaks riskierandid juhtudel, kus täielikku vastavust ei ole võimalik äripiirangute tõttu saavutada.

4.2 Rakenduse omanik (kui määratud)

4.2.1 Tuvastab rakenduse spetsiifilised turbevajadused süsteemi valiku või projekti algatamise käigus.

4.2.2 Kontrollib, et peamised funktsioonid, nagu sisselogimiskaitse, krüptimine ja tegevuslogid, on olemas.

4.2.3 Osaleb kasutuselevõtueelsetes ülevaatustes ja kinnitab, et turbekontrollid vastavad ärivajadustele.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Tegevjuht peab käesoleva poliitika läbi vaatama vähemalt üks kord kalendriaastas, et:

9.1.1 kajastada regulatiivsete nõuete muudatusi (nt GDPR, NIS2, DORA);

9.1.2 võtta arvesse uusi või esilekerkivaid ohte ja ründetehnikaid;

9.1.3 ajakohastada sõnastust ja nõudeid vastavalt platvormide, tarnijate või arendusmeetodite muutustele.

9.2 Vahepealsed läbivaatused tuleb teha ka juhul, kui:

9.2.1 võetakse kasutusele uusi rakendusi;

9.2.2 olemasolevatele rakendustele tehakse olulisi uuendusi või liidestusi;

9.2.3 toimub rakendusega seotud intsident või rikkumine;

9.2.4 väliste teadete või valdkondlike hoiatuste põhjal tuvastatakse uusi riske.

9.3 Kõik käesoleva poliitika muudatused peavad olema:

9.3.1 tegevjuhi poolt heaks kiidetud;

9.3.2 dokumenteeritud koos versiooniajaloo ja muudatuse põhjusega;

9.3.3 edastatud kõigile töötajatele, arendajatele ja tarnijatele, kes osalevad rakenduste haldamises;

9.3.4 turvaliselt säilitatud auditi ja vastavuse eesmärgil.

10. Seotud poliitikad ja seosed

10.1 Käesolevat poliitikat toetavad otseselt järgmised VKEdele kohandatud turbepoliitikad ning see aitab kaasa nende rakendamisele:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määrab vastutuse rakenduste heakskiitmise, poliitika rakendamise ja tarnijate haldamise eest.

10.1.2 P4S – Juurdepääsukontrolli poliitika: tagab, et juurdepääs rakendustele on kooskõlas vähimate õiguste põhimõtte ja seansikontrolli põhimõtetega.

10.1.3 P8S – Infoturbeteadlikkuse ja koolituse poliitika: tagab, et kasutajad ja arendajad on koolitatud rakendustega seotud ohtude tuvastamiseks ja neist teatamiseks.

10.1.4 P17S – Andmekaitse ja privaatsuspoliitika: sätestab andmekaitsemeetmed, mida peab rakendama iga rakendus, mis töötleb isikuandmeid.

10.1.5 P14S – Andmete säilitamise ja kõrvaldamise poliitika: reguleerib, kuidas rakenduse loodud logisid, varukoopiaid ja tundlikke andmeid tuleb säilitada, arhiveerida ja turvaliselt hävitada.

10.1.6 P30S – Intsidentidele reageerimise poliitika: kirjeldab samme rakendustega seotud turbesündmuste tuvastamiseks, neist teatamiseks ja nende ohjamiseks.

10.2 Koos tagavad need poliitikad, et rakenduste turve on täielikult integreeritud organisatsiooni infoturbe juhtimissüsteemi ning on auditivalmis.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab, et organisatsioon kehtestaks operatiivsed kontrollimeetmed infoturberiskide käsitlemiseks, sealhulgas rakenduste ja tarkvarasüsteemidega seotud riskide jaoks.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.25 – soovitab rakendada turvalise kavandamise, arendamise ja koodi läbivaatuse tavasid kõigis rakendustes, sealhulgas tarnijate pakutavates rakendustes.

11.2.2 Kontroll 8.26 – soovitab rakenduste turbekontrollide ametlikku testimist, eelkõige juurdepääsukontrolli, sisendi valideerimise ja seansihalduse valdkondades.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – määratleb nõuded arendajate testimisele, koodianalüüsile ja rakenduste dünaamilisele skannimisele enne juurutamist.

11.3.2 SI-10 – käsitleb levinud tarkvarapuuduste tuvastamist ja ennetamist, rõhutades arendajate teadlikkust ja tehnilisi kaitsemeetmeid.

11.4 EL GDPR (2016/679)

11.4.1 Artikkel 25 – „andmekaitse kavandamisel ja vaikimisi andmekaitse“ nõuab, et isikuandmeid töötlevate rakenduste põhilahendusse oleks integreeritud andmekaitse ja turve.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(a) ja (e) – nõuab, et olulised ja tähtsad üksused rakendaksid tehnilisi meetmeid rakenduste kaitsmiseks ja tarkvaraga seotud riskide tuvastamiseks.

11.6 EL DORA (2022/2554)

11.6.1 Artikkel 9(2)(c), 10(2)(c) – nõuab, et finantssektori VKEd rakendaksid rakendustaseme turbekontrolle ja teeksid regulaarseid hindamisi digitaalse operatiivse toimepidevuse säilitamiseks.

11.7 COBIT 2019

11.7.1 BAI03 – „Lahenduste tuvastamise ja loomise juhtimine“ suunab turvalise tarkvara arendamist või hankimist kooskõlas riski-, vastavus- ja ärinõuetega, sealhulgas piiratud ressurssidega VKE-keskkondades.