					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P25					Dokumendi pealkiri: **Rakendusturbe nõuete 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 regulatsioonidele

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	—
ISO/IEC 27002:2022	Kontrollimeetmed 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
EL GDPR	Artikkel 25, 32	—
EL NIS2	Artikkel 21(2)(f), 23	—
EL DORA	Artikkel 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud rakenduskihi turbenõuded tarkvarale, mida organisatsioon arendab, hangib, integreerib või kasutusele võtab. See tagab, et kõik rakendused kavandatakse, juurutatakse ja hallatakse kooskõlas turvalise arenduse põhimõtete, regulatiivsete kohustuste ja organisatsiooni riskivalmidusega.

1.2 Poliitika nõuab turbe käsitlemist kogu rakenduse elutsükli jooksul, hõlmates kasutajate autentimist, andmete töötlemist, liideste kaitset ning turvalist suhtlust API-de ja teenustega.

1.3 Käesoleva poliitika rakendamise eesmärk on vältida tarkvara turvanõrkuste lisandumist, kaitsta tundlikke andmeid ning tagada jälgitavus ja vastupidavus ärakasutamisele ning väärkasutusele.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmiste objektide ja osapoolte suhtes:

2.1.1 Organisatsioonis arendatud või väliselt hangitud rakendused, sealhulgas SaaS-lahendused ja eritellimusel loodud tööriistad

2.1.2 Rakendused, mis toetavad kriitilisi äritegevusi, kliendipoolset juurdepääsu või reguleeritud andmete töötlemist

2.1.3 Arendus-, DevOps-, kvaliteeditagamise, toote- ja turvameeskonnad

2.1.4 Kolmandate osapoolte arendajad, tarkvaratarnijad ja integratsioonipartnerid, kellel on juurdepääs organisatsiooni rakendustele või API-dele

2.2 Poliitika kehtib kõigis keskkondades: arendus-, test-, eeltootmis-, tootmis- ja taastekeskkonnas, sõltumata sellest, kas lahendus asub kohapealses taristus, privaatses andmekeskuses või avalikus pilvekeskkonnas.

3. Eesmärgid

3.1 Määratleda funktsionaalsed ja mittefunktsionaalsed turbenõuded miinimumtasemel, mida peavad täitma kõik rakendused sõltumata arendusmetoodikast või tehnoloogiapakist.

3.2 Tagada rakenduskihi kaitsemeetmete lõimimine, sealhulgas sisendite valideerimine, väljundi kodeerimine, veatöötlus ja seansside turve.

3.3 Nõuda autentimise, autoriseerimise ja juurdepääsukontrolli mehhanismide turvalist rakendamist kooskõlas organisatsiooni identiteedi- ja juurdepääsuhalduse poliitikatega.

3.4 Kehtestada nõue tagada API-de, veebiliideste ja kolmandate osapoolte komponentidega suhtluse turvalisus, kasutades heakskiidetud protokolle ja kontrollimeetmeid.

3.5 Võimaldada turvanõrkuste varajane tuvastamine ja leevendamine staatilise ja dünaamilise analüüsi, koodiülevaatuse ning ohumudeldamise kaudu.

3.6 Kaitsta tundlikke andmeid kooskõlas regulatiivsete nõuetega, rakendades krüpteerimist, klassifitseerimist ja andmete säilitamise reegleid.

3.7 Tagada rakenduste turbeoleku pidev valideerimine pärast kasutuselevõttu testimise, seire ja auditeerimisvalmiduse kaudu.

4. Rollid ja vastutused

4.1 Infoturbejuht (CISO)

4.1.1 Vastutab käesoleva poliitika eest ja tagab selle kooskõla organisatsiooni infoturbe strateegia ning riskitasemega.

4.1.2 Kinnitab rakendusturbe nõuded ja tagab kohustuslike kontrollimeetmete rakendamise arendus- ja hankefunktsioonides.

4.2 Rakendusturbe juht / DevSecOpsi juht

4.2.1 Määratleb rakenduste komponentide miinimumtaseme turbekontrollid ja testimismetoodikad.

4.2.2 Juhib selliste tööriistade nagu SAST, DAST, IAST ja SCA turvalist lõimimist tarkvara tarneahelasse.

4.2.3 Haldab rakendusturbe nõuete kontroll-loendit ja valideerimiskriteeriume.

[... 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 või sagedamini järgmiste asjaolude ilmnemisel:

9.1.1 Kriitiliste turvanõrkuste avalikustamine, mis mõjutab laialdaselt kasutatavaid raamistikke või sõltuvusi

9.1.2 Rakendusturvet puudutavate regulatiivsete kohustuste uuendused, näiteks NIS2 või DORA

9.1.3 Olulised muudatused organisatsiooni tarkvaraarenduse tavades, tööriistades või pilvearhitektuuris

9.1.4 Siseauditite või väliste penetratsioonitestide leiud

9.2 Läbivaatamist juhib rakendusturbe juht koostöös CISO, DevOpsi inseneeria, õigus-, hanke- ja kvaliteeditagamise juhtidega.

9.3 Kõik muudatused peavad olema versioonihaldusega kajastatud ISMS-i dokumendihalduse registris ning edastatud kõigile mõjutatud arendus- ja tootemeeskondadele.

9.4 Asendatud versioone tuleb jälgitavuse, auditeeritavuse ja rikkumiste uurimise toetamiseks arhiveerida vähemalt kolmeks aastaks.

10. Seotud poliitikad ja seosed

10.1 P1 – Infoturbe poliitika. Määratleb süsteemide ja andmete kaitse aluspõhimõtted, mille raames tuleb rakendada rakenduskihi kontrollimeetmeid volitamata juurdepääsu, andmelekkete ja ärakasutamise vältimiseks.

10.2 P4 – Juurdepääsukontrolli poliitika. Määratleb identiteedi- ja seansihalduse standardid, mida kõik rakendused peavad rakendama, sealhulgas tugeva autentimise, vähima privileegi põhimõtte ja juurdepääsu läbivaatamise nõuded.

10.3 P5 – Muudatuste juhtimise poliitika. Reguleerib rakenduskoodi ja seadistuste edendamist tootmiskeskkonda, tagades, et volitamata või testimata muudatused blokeeritakse.

10.4 P17 – Andmekaitse ja privaatsuse poliitika. Nõuab, et rakendused rakendaksid lõimitud andmekaitse põhimõtet ning tagaksid isikuandmete ja tundlike andmete õiguspärase töötlemise, krüpteerimise ja säilitamise kõigis keskkondades.

10.5 P24 – Turvalise arenduse poliitika. Annab laiema raamistiku turbe lõimimiseks SDLC-sse; käesolev poliitika määratleb selle raames konkreetsed nõuded ja tehnilised kontrollimeetmed, mis tuleb rakenduskihis rakendada.

10.6 P30 – Intsidendihalduse poliitika. Nõuab rakendusturbe intsidentide struktureeritud käsitlemist, sealhulgas pärast kasutuselevõttu või penetratsioonitestide käigus tuvastatud turvanõrkuste puhul, ning määratleb eskaleerimise, ohjamise ja taastamise korra.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001:2022

11.1.1 Punkt 8.1 – Tegevuse planeerimine ja ohje: nõuab rakendusturbe lõimimist protsessidesse ja süsteemidesse, et tagada konfidentsiaalsus, terviklus ja käideldavus.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrollimeetmed 8.25–8.26: kirjeldavad ootusi rakenduskihi turbele, sealhulgas turvalise programmeerimise tavasid, ohumudeldamist, arhitektuurseid kontrollimeetmeid ja kolmanda osapoole tarkvara valideerimist.

11.2.2 Lisa A kontrollimeede 8.25 – Turvaline arenduse elutsükkel: nõuab turbe lõimimist kogu rakenduse elutsükli jooksul.

11.2.3 Lisa A kontrollimeede 8.26 – Rakendusturbe nõuded: nõuab tehniliste kontrollimeetmete määratlemist ja rakendamist, et kaitsta rakendusi väärkasutuse ja kompromiteerimise eest.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Arendaja teostatav turbetestimine ja hindamine: nõuab arenduse käigus staatilist, dünaamilist ja penetratsioonitestimist.

11.3.2 SA-15 – Arendusprotsess, standardid ja tööriistad: kehtestab turvalise rakenduse arenduse formaalsed standardid.

11.3.3 SI-10 – Teabesisendi valideerimine: nõuab kontrollimehhanisme sisestus- ja parsimisrünnete vältimiseks.

11.4 EL GDPR (2016/679)

11.4.1 Artikkel 25 – Lõimitud andmekaitse ja vaikimisi andmekaitse: nõuab andmekaitse ja privaatsuse lõimimist rakenduse loogikasse ja töövoogudesse.

11.4.2 Artikkel 32 – Töötlemise turvalisus: nõuab asjakohaseid tehnilisi meetmeid, näiteks sisendi valideerimist, krüpteerimist ja turvalist juurdepääsukontrolli.

11.5 EL NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(f): nõuab turvanõrkuste käsitlemist ja turvalise rakenduse elutsükli tavasid elutähtsate ja oluliste üksuste jaoks.

11.5.2 Artikkel 23 – Turvaintsidentidest teatamine: nõuab rakenduskihi logimise ja seire võimekust oluliste intsidentide tuvastamiseks ja raporteerimiseks.

11.6 EL DORA (2022/2554)

11.6.1 Artikkel 9 – IKT-riski juhtimine: kohustab finantssektori üksusi tagama, et rakendused on turvalised, testitud ja küberohtude suhtes vastupidavad.

11.6.2 Artikkel 11 – IKT-vahendite testimine: soodustab kriitiliste rakenduste ja teenuste perioodilist penetratsioonitestimist ning punase meeskonna testimist.

11.7 COBIT 2019

11.7.1 BAI03 – Lahenduste tuvastamise ja loomise juhtimine: kehtestab kavandamise ja kontrolli nõuded rakenduste arendamisel.

11.7.2 BAI09 – Rakenduste juhtimine: rõhutab kasutusel olevate rakenduste turvalist haldust, seiret ja täiustamist.

11.7.3 DSS05 – Turbeteenuste juhtimine: seob rakenduste kaitse organisatsiooni laiemate turvatoimingute ja kontrollimeetmetega.