					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P40					Dokumendi pealkiri: **Turbetestimise ja punase meeskonna 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	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
EL GDPR	Art. 32(1)(d)	
EL NIS2	Art. 21(2)(f)	
EL DORA	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Eesmärk

1 Organisatsioon kehtestab struktureeritud programmi oma võrkude, süsteemide ja rakenduste regulaarseks turbetestimiseks, sealhulgas haavatavuste hindamiseks, penetratsioonitestimiseks ja punase meeskonna harjutusteks, et täita NIS2 artikli 21 lõike 2 punkti f nõuet küberturberiskide juhtimise meetmete tõhususe hindamiseks.

1.1 Organisatsioon peab tagama, et tehniliste ja korralduslike meetmete nõrkused tuvastatakse ennetavalt ning kõrvaldatakse kontrollitud testimise kaudu, et organisatsiooni turbeolekut pidevalt parandada.

2. Kohaldamisala

2 Käesolev poliitika hõlmab kõiki organisatsiooni omandis või hallatavaid kriitilisi infosüsteeme, rakendusi ja neid toetavat taristut. Poliitika hõlmab ka füüsilise turbe testimist ulatuses, milles see on seotud küberturbega, näiteks sotsiaalse manipulatsiooni või füüsilise sissetungi testimist, kui see kuulub punase meeskonna tegevusulatusse.

2.1 Poliitika kehtib sisemistele turvameeskondadele, lepingulistele välistele turbetestimise teenuseosutajatele ning asjakohastele süsteemi- ja rakenduseomanikele. Kõik testimistegevused peavad olema autoriseeritud ja toimuma käesolevas poliitikas sätestatud korras, et vältida soovimatuid häireid.

3. Eesmärgid

3 Organisatsioon peab perioodilise testimise ja simulatsioonide abil kontrollima rakendatud küberturbe kontrollimeetmete, sealhulgas tehniliste, tegevuslike ja organisatsiooniliste kontrollimeetmete tõhusust kooskõlas NIS2 nõudega mõõta nende tulemuslikkust.

3.1 Testimisega tuleb tuvastada haavatavused ja puudujäägid, mis võivad tavapärastes tegevusprotsessides märkamata jääda, sealhulgas nullpäeva haavatavused või konfiguratsioonivead, kasutades punase meeskonna harjutuste raames realistlikke ründestsenaariume enne, kui vastased neid ära kasutavad.

3.2 Testitulemuste aruandluse kaudu tuleb anda juhtkonnale kindlus ja rakendatavad soovitused, et toetada teadlikke riskikäsitluse otsuseid ning turbeprogrammi pidevat täiustamist.

4. Rollid ja vastutused

4 Turbetestimise koordinaator (STC): infoturbe juht nimetab turbetestimise koordinaatori, kes vastutab kõigi turbetestimise tegevuste kavandamise ja järelevalve eest. Ta tagab, et testid on selgelt piiritletud, autoriseeritud ning et tulemused raporteeritakse ja nende põhjal tegutsetakse.

4.1 Sisemine turvameeskond (Blue Team): osaleb testides koostöös, näiteks annab teavet tegevusulatuse määratlemiseks ja jälgib testide ajal süsteeme. Punase meeskonna harjutuste korral reageerib Blue Team simuleeritud rünnetele ning hinnatakse nende tuvastus- ja reageerimisvõimekust.

4.2 Punane meeskond / penetratsioonitestijad: võivad olla organisatsiooni sisemine ründava turbe meeskond või välised konsultandid. Nad viivad testid läbi kokkulepitud tegutsemisreeglite alusel, dokumenteerivad kõik avastatud haavatavused ja ärakasutamise teekonnad ning tagavad konfidentsiaalsuse.

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

9. Seire ja audit

9 STC peab pidama kalendrit ja logi kõigi tehtud turbetestimise tegevuste kohta. Logi peab sisaldama kuupäeva, tegevusulatust, testi läbiviijat ja tulemuste kokkuvõtet. Seda tuleb regulaarselt üle vaadata, et tagada nõutud ajakava järgimine, näiteks et ükski kriitiline süsteem ei jääks testimata kauemaks, kui aastane tsükkel lubab.

9.1 Testimise leidude kõrvaldamise edenemist tuleb seirata ja sellest tuleb kord kuus aru anda. Avatud kõrge tõsidusega küsimused tuleb juhtkonna koosolekutel läbi vaadata kuni nende sulgemiseni.

9.2 Siseaudit või sõltumatu audiitor peab turbetestimise programmi igal aastal läbi vaatama, et kontrollida, kas testid on nõuetekohaselt autoriseeritud, läbi viidud ja aruandlusega kaetud, kas kriitilised leiud on käsitletud ning kas programm vastab regulatiivsetele ootustele. Näiteks võivad audiitorid kontrollida, kas enne uue veebiteenuse kasutuselevõttu tehti nõutud penetratsioonitest. Kõik kõrvalekalded peavad kaasa tooma parandusmeetmete plaanid.

10. Läbivaatamine ja ajakohastamine

10 Käesolev poliitika ja üldine testimisplaan tuleb läbi vaadata vähemalt kord aastas. Läbivaatamisel tuleb arvesse võtta muutusi ohumaastikus, näiteks uute ründetehnikate esilekerkimist, mida olemasolev testimine ei kata, ning vastavalt kohandada tegevusulatust või sagedust.

10.1 Pärast iga olulist küberturbeintsidenti või rikkumist tuleb käesolev poliitika uuesti läbi vaadata, et hinnata, kas täiendav või sagedasem testimine oleks aidanud juhtumit ennetada või tuvastada. Seejärel tuleb poliitikat ajakohastada, et vajalikud muudatused sisse viia, näiteks lisades punase meeskonna harjutustesse uue stsenaariumi täheldatud ründemustrite põhjal.

10.2 Käesoleva poliitika muudatused peab heaks kiitma infoturbe juht ning juhatus peab need teadmiseks võtma. Kõiki asjakohaseid töötajaid tuleb muudatustest teavitada ning väliseid testimispartnereid tuleb teavitada juhul, kui muudatus mõjutab nende töötingimusi.

11. Seotud poliitikad ja seosed

11.1 P06 – Riskijuhtimise poliitika. Testimise väljundid toetavad riskide hindamist ja riskikäsitlust.

11.2 P22 – Logimise ja seire poliitika. Valideerib harjutuste ajal tuvastuskatvust.

11.3 P24 – Turvalise arenduse poliitika. Lõimib testimise leiud SDLC kontrollimeetmetesse.

11.4 P25 – Rakendusturbe nõuete poliitika. Tagab, et nõuded kajastavad testimisest saadud õppetunde.

11.5 P30 – Intsidentidele reageerimise poliitika. Punase meeskonna stsenaariumid täiustavad tööjuhiseid ja reageerimist.

11.6 P31 – Tõendite kogumise ja kohtuekspertiisi poliitika. Käsitleb testimise käigus artefaktide turvalist kogumist.

11.7 P32 – Talitluspidevuse ja katastroofitaaste poliitika. Harjutused kontrollivad vastupidavust rünnaku korral.

11.8 P33 – Auditi ja vastavusseire poliitika. Tagab turbetestimise programmi tõhususe sõltumatu järelevalve.

12. Viited

12.1 NIS2 direktiiv (EL 2022/2555), artikkel 21 lõige 2 punkt f (küberturberiskide juhtimise meetmete tõhususe hindamise poliitikad ja protseduurid)

12.2 Komisjoni rakendusmäärus (EL) 2024/2690, lisa punkt 7 (küberturbe meetmete seire, testimise ja tõhususe hindamise nõuded)

12.3 ENISA tehnilised suunised (2025) – lisa turbetestimise ja auditi kohta (suunised küberturbe õppuste ja tehniliste testide läbiviimiseks)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Valdkonna parimad praktikad: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (finantssektori punase meeskonna raamistikud viitamiseks)