					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P19					Dokumendi pealkiri: **Haavatavuste ja paikade halduse 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/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Tehniliste haavatavuste süsteemne käsitlemine; turbekontrollide pidev tõhusus.
ISO/IEC 27002:2022	Kontrollimeetmed 8.8, 8.9, 5	Rakendusjuhised paikamiseks, haavatavuste skannimiseks, tarkvara tervikluseks, turvaliseks konfiguratsiooniks ja vararegistri pidamiseks.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Sagedased skannimised, puuduste kõrvaldamine ja konfiguratsioonihaldus peavad olema rakendatud.
ELi GDPR	Artikkel 32, põhjendus 49	Tehnilised meetmed õigeaegseks paikamiseks, haavatavuste käsitlemiseks ja turbe toimepidevuse tagamiseks.
ELi NIS2	Artikkel 21(2)(d)	Haavatavuste tuvastamine, neile reageerimine ja nende maandamine kõrge küberhügieeni tagamiseks.
ELi DORA	Artiklid 8, 10(2)(f)	IKT-haavatavuste õigeaegne kõrvaldamine; pidevad ohupõhised hindamised.
COBIT 2019	DSS05.02, DSS01.03, MEA	Tehniliste nõrkuste skannimine, jälgimine ja maandamine; ärakasutamise seire; tõhususe auditeerimine, sh paikamise staatus.

1. Eesmärk

1.1 Käesolev poliitika kehtestab organisatsiooni kohustuslikud nõuded kõigi infoturbe juhtimissüsteemi (ISMS) kohaldamisalasse kuuluvate infosüsteemide ja varade tehniliste haavatavuste ning tarkvarapuuduste tuvastamiseks, klassifitseerimiseks, kõrvaldamiseks ja seireks.

1.2 See tagab, et kõiki teadaolevaid haavatavusi hinnatakse ja käsitletakse riskipõhiselt ning õigeaegselt koordineeritud paikamise, konfiguratsioonimuudatuste või kompenseerivate kontrollimeetmete kaudu kooskõlas äritegevuse vajaduste ja vastavuskohustustega.

1.3 Käesolev poliitika toetab vastavust standardi ISO/IEC 27001 lisa A kontrollimeetmele 8.8 ja ISO/IEC 27002 juhistele ning käsitleb DORA artikli 8, NIS2 artikli 21, GDPR artikli 32 ja COBIT 2019 DSS- ja APO-valdkondade regulatiivseid nõudeid.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigi infosüsteemide, varade ja keskkondade suhtes, mis salvestavad, töötlevad või edastavad andmeid ning millele kohaldub ISMS-i juhtimine, sealhulgas:

2.1.1 operatsioonisüsteemid, rakendused, võrguseadmed, püsivara, pilveplatvormid, API-d ja kolmanda osapoole tarkvara.

2.1.2 süsteemid arendus-, test-, tootmis-, varundus- ja katastroofitaastekeskkondades.

2.1.3 lõppseadmed, serverid, asjade interneti (IoT) seadmed, virtualiseerimistaristu ja konteinerid.

2.2 See on siduv järgmistele osapooltele:

2.2.1 sisemine personal: IT-administraatorid, süsteemiinsenerid, rakendusearendajad, turbeanalüütikud ja taristumeeskonnad.

2.2.2 välised osapooled: töövõtjad, hallatud teenusepakkujad (MSP-d), tarkvaratarnijad ja süsteemiintegraatorid, kellel on tehniline vastutus kohaldamisalasse kuuluvate varade eest.

2.3 Poliitika hõlmab haavatavuste ja paikamise kogu elutsüklit, sealhulgas:

2.3.1 skannimine ja tuvastamine

2.3.2 riskide klassifitseerimine ja prioriseerimine

2.3.3 paikade hankimine, testimine, juurutamine ja tagasipööramine

2.3.4 erandite käsitlemine ja kompenseerivate kontrollimeetmete kavandamine

2.3.5 logimine, aruandlus ja auditijälje jälgitavus

3. Eesmärgid

3.1 Tagada, et kõik teadaolevad haavatavused tuvastatakse, hinnatakse ja kõrvaldatakse viisil, mis minimeerib riskipositsiooni ja on kooskõlas tegevusprioriteetidega.

3.2 Kehtestada ühtsed, kogu organisatsiooni hõlmavad protsessid haavatavuste skannimiseks, tõsiduse klassifitseerimiseks (nt CVSS) ja paikamise haldamiseks, sealhulgas erakorraliseks käsitlemiseks ja tagasipööramise kavandamiseks.

3.3 Võimaldada turvalist konfiguratsioonihaldust kooskõlas kõvendamise lähtealustega, muudatuste juhtimise praktikatega ja reaalajas ohuteabega.

3.4 Tagada mõõdetav vastavus regulatiivsetele ja standardipõhistele kontrollimeetmetele, mis käsitlevad süsteemi terviklust, paikamisdistsipliini ja puuduste õigeaegset kõrvaldamist.

3.5 Määratleda vastutus ja aruandekohustus kogu haavatavuste halduse elutsükli ulatuses, tagades, et kõik sidusrühmad tegutsevad määratletud SLA-de piires ja esitavad aruandekohustust toetavaid kontrollmõõdikuid.

3.6 Tagada auditivalmidus ja suurendada toimepidevust esilekerkivate ohtude vastu, sealhulgas nullpäeva-haavatavused, aktiivsed ärakasutusahelad ja olulised tarnijate turvateated.

4. Rollid ja vastutused

4.1 infoturbe juht

4.1.1 Vastutab poliitika eest ja tagab selle lõimimise ISMS-i.

4.1.2 Määratleb organisatsiooni riskipositsiooni ning tagab kooskõla regulatiivsete nõuete ja kontrolliootustega.

4.2 haavatavuste halduse juht / turbeoperatsioonide juht

4.2.1 Tagab tervikliku järelevalve haavatavuste ja paikamise halduse üle.

4.2.2 Koordineerib skannimisgraafikuid, prioriseerimismudeleid ja kõrvaldamise tähtaegu.

4.2.3 Haldab haavatavuste registrit ja teeb koostööd kompenseerivate kontrollimeetmete hindamisel.

[... 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 järgmiste asjaolude ilmnemisel:

9.1.1 olulised regulatiivsed muudatused (nt DORA või NIS2 muudatused)

9.1.2 muudatused haavatavuste prioriseerimise raamistikus (nt CVSS-i uuendused)

9.1.3 olulised muutused IT-keskkonnas (nt pilvemigratsioon, EDR-i ulatuslik ümberkujundamine)

9.1.4 suure mõjuga rikkumised või välised teated, mis nõuavad poliitika tugevdamist

9.2 Läbivaatamise viib läbi infoturbe juht koostöös turbeoperatsioonide, riskijuhtimise ja taristu eest vastutava juhtkonnaga.

9.3 Poliitikamuudatused peavad olema:

9.3.1 dokumenteeritud ISMS-i dokumentide kontrolli registris

9.3.2 läbi vaadatud ja heaks kiidetud tippjuhtkonna poolt

9.3.3 edastatud kõigile mõjutatud sidusrühmadele, sealhulgas kolmandatest osapooltest volitatud töötlejatele

9.4 Ajaloolisi versioone tuleb säilitada turvaliselt auditi ja aruandekohustuse eesmärgil.

10. Seotud poliitikad ja seosed

10.1 P1 - infoturbepoliitika. Määratleb üldise kohustuse kaitsta süsteeme ja andmeid, sealhulgas haavatavuste ennetava halduse ja tarkvara tervikluse tagamise.

10.2 P5 - muudatuste haldamise poliitika. Reguleerib kõiki paikade juurutamisi ja konfiguratsioonimuudatusi ning nõuab dokumenteerimist, testimist, heakskiitu ja tagasipööramisprotseduure, mis täiendavad haavatavuste kõrvaldamise protsesse.

10.3 P6 - riskijuhtimise poliitika. Toetab kõrvaldamata haavatavuste klassifitseerimist ja käsitlemist struktureeritud riskihindamiste, mõjuhindamise ja jääkriski aktsepteerimise protseduuride kaudu.

10.4 P12 - varahalduse poliitika. Tagab süsteemide korrektse registreerimise ja klassifitseerimise, võimaldades järjepidevat haavatavuste skannimist, omanikuvastutuse määramist ja paikamise halduse katvust kogu elutsükli jooksul.

10.5 P22 - logimise ja seire poliitika. Määratleb nõuded sündmuste tuvastamiseks ja auditijälje loomiseks. Käesolev poliitika toetab nähtavust paikamistegevuste, autoriseerimata muudatuste ja teadaolevaid haavatavusi sihtivate ärakasutamiskatsete üle.

10.6 P30 - intsidentidele reageerimise poliitika (P30). Määratleb eskaleerimisprotokollid ja ohjeldusstrateegiad ärakasutatud haavatavuste, rikkumiste uurimise ja käesoleva poliitikaga kooskõlas olevate parandusmeetmete jaoks.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001: punkt 8.1 - tegevuse planeerimine ja kontroll: nõuab tehniliste haavatavuste süsteemset käsitlemist, et tagada turbekontrollide pidev tõhusus.

11.2 ISO/IEC 27002:2022 - kontrollimeetmed 8.8, 8.9, 5: annab rakendusjuhised paikamiseks, haavatavuste skannimiseks, tarkvara tervikluse tagamiseks ning lõimimiseks turvalise konfiguratsiooni ja vararegistriga.

11.3 NIST SP 800-53 Rev.5: RA-5 - haavatavuste seire ja skannimine: nõuab sagedast skannimist ja kõrvaldamise jälgimist. SI-2 - puuduste kõrvaldamine: nõuab puuduste kiiret hindamist ja maandamist olemasolevate paikade või muude meetmetega. CM-2 / CM-6 - konfiguratsioonihalduse lähtetasemed ja kontrollimeetmed: loovad aluse turvalistele süsteemikonfiguratsioonidele, mis on seotud paikamise rakendamisega.

11.4 ELi GDPR (2016/679): artikkel 32 - töötlemise turvalisus: nõuab asjakohaste tehniliste meetmete rakendamist, näiteks õigeaegset paikamist ja haavatavuste käsitlemist, et tagada konfidentsiaalsus ja süsteemide toimepidevus. Põhjendus 49: julgustab üksusi rakendama ennetavaid kontrollimeetmeid teadaolevate ohtude vastu, et toetada turvalisust ja talitluspidevust.

11.5 ELi NIS2 direktiiv (2022/2555): artikkel 21(2)(d): kohustab olulisi ja tähtsaid üksusi tuvastama süsteemide haavatavusi, neile reageerima ja neid maandama ning hoidma kõrget küberhügieeni taset.

11.6 ELi DORA (2022/2554): artikkel 8 - IKT-riskide juhtimine: nõuab finantssüsteemides kasutatavate info- ja sidetehnoloogiate haavatavuste tuvastamist ja õigeaegset kõrvaldamist. Artikkel 10(2)(f): rõhutab pidevaid ohupõhiseid haavatavuste hindamisi ja paikamist kui osa operatiivsest toimepidevusest.

11.7 COBIT 2019: DSS05.02 - turbehaavatavuste haldamine: suunab organisatsioone teadaolevaid tehnilisi nõrkusi skannima, jälgima ja maandama. DSS01.03 - taristu seire: tagab süsteemide jälgimise ärakasutamise või nõrkuse tunnuste suhtes. MEA03 - vastavuse seire, hindamine ja auditeerimine: nõuab kontrollimeetmete tõhususe regulaarset auditeerimist, sealhulgas paikamise staatuse ja erandite käsitlemise osas.