					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P19S					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/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	
ISO/IEC 27002:2022	Kontrollimeetmed 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EL NIS2	Artiklid 21(2)(d), 21(2)(e)	
EL DORA	Artiklid 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
EL GDPR	Artikkel 32(1)(b)	

1. Eesmärk

1.1 Käesolev poliitika määratleb, kuidas organisatsioon tuvastab, hindab ja maandab haavatavusi süsteemides, rakendustes ja taristus.

1.2 Käesoleva poliitika eesmärk on vähendada küberriski, tagades õigeaegse paikamise ja riskipõhise puuduste kõrvaldamise viisil, mis on sobiv väikeste ja keskmise suurusega ettevõtete (VKE-de) jaoks.

1.3 Käesolev poliitika toetab vastavust ISO/IEC 27001:2022 sertifitseerimisnõuetele ning aitab täita GDPR-ist, NIS2-st ja DORA-st tulenevaid regulatiivseid kohustusi, nõudes tehniliste haavatavuste ennetavat haldamist.

1.4 Organisatsioon tunnistab, et paikamata süsteemid kujutavad endast olulist ohtu infoturbele ning neid tuleb käsitleda süsteemselt ja viivituseta.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub järgmisele:

2.1.1 kõik organisatsiooni kasutatavad serverid, lauaarvutid, sülearvutid, mobiilsed seadmed, võrguseadmed ja pilvekeskkonnas majutatud platvormid;

2.1.2 kõik äritegevuses kasutatavad operatsioonisüsteemid, kolmanda osapoole tarkvara, pistikprogrammid ja rakendused;

2.1.3 sisemine IT-personal või välised teenuseosutajad, kes vastutavad süsteemide hoolduse, uuenduste või seire eest;

2.1.4 organisatsiooni hallatav või organisatsiooni nimel hallatav kohandatud arenduskood või püsivara.

2.2 Poliitika hõlmab nii organisatsiooni poolt vahetult hallatavat taristut kui ka süsteeme, mida haldavad lepingulised tarnijad või majutusteenuse osutajad.

3. Eesmärgid

3.1 Tuvastada ja hinnata teadaolevaid haavatavusi kõigis IT-varades õigeaegselt ja järjepidevalt.

3.2 Rakendada paigad ja tarkvarauuendused vastavalt nende kriitilisusele ning riskile organisatsiooni tegevusele või isikuandmetele.

3.3 Ennetada tehniliste nõrkuste ärakasutamist, mis võib põhjustada teenusekatkestusi, isikuandmetega seotud rikkumisi või õigusnormidele mittevastavust.

3.4 Säilitada täpsed kirjed rakendatud paikade, lahendamata probleemide ja erandite kohta, et tagada auditivalmidus.

3.5 Kasutada organisatsiooni suurusele ja tegevuse keerukusele sobivaid tööriistu ja protsesse, kahjustamata seejuures tõhusust.

3.6 Toetada õigusnormidele vastavust, sealhulgas GDPR artikli 32 ja ISO lisa A kontrollimeetme 8 nõudeid.

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 Vastutab üldiselt selle eest, et paikade ja haavatavuste halduse tegevused oleksid rakendatud.

4.1.2 Kiidab heaks riskierandid juhtudel, kui paiku ei ole võimalik rakendada, ning vaatab läbi nendega seotud maandamismeetmed.

4.1.3 Vaatab läbi paikamise staatuse aruanded ja tagab ressursside olemasolu paikamiskohustuste täitmiseks.

4.2 IT-toe teenuseosutaja / sisemine IT-vastutaja

4.2.1 Seirab süsteemide haavatavusi ja saadaolevaid paiku, kasutades tarnijate teavitusi, ohuteavet ja operatsioonisüsteemi tasandi teavitusi.

4.2.2 Rakendab operatsioonisüsteemide, püsivara ja rakenduste uuendused määratud tähtaegade jooksul.

4.2.3 Hoiab ametlikku paikade logi ning dokumenteerib lahendamata või edasi lükatud uuendused.

4.2.4 Viib läbi kriitiliste uuenduste testimise ja ajastamise, et minimeerida häireid tegevuses.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Iga-aastane läbivaatamine

9.1.1 Käesolev poliitika tuleb vähemalt kord aastas läbi vaadata tegevjuhi poolt, kaasates IT-teenuseosutaja ja andmekaitsekoordinaatori sisendi.

9.2 Läbivaatamise alused

9.2.1 Vahepealne läbivaatamine tuleb teha, kui:

9.2.1.1 mõni oluline haavatavus või ärakasutamine mõjutab kohaldamisalasse kuuluvaid süsteeme;

9.2.1.2 toimuvad olulised süsteemi- või tarkvaramuudatused;

9.2.1.3 audit tuvastab puudujääke paikamisprotsessides;

9.2.1.4 registreeritakse paikamisega seotud intsident või rikkumine.

9.3 Poliitika versioonihaldus

9.3.1 Kõik uuendused tuleb registreerida versioonilogis koos muudatuste kokkuvõttega.

9.3.2 Muudatustest tuleb teavitada mõjutatud töötajaid.

9.3.3 Aegunud versioonid tuleb arhiveerida piiratud juurdepääsuga.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toetab mitut teist VKE poliitikat ja sõltub neist:

10.1.1 P12S – Varahalduse poliitika: määratleb süsteemide omandivastutuse ja klassifitseerimise, tagades, et kõik paikamist vajavad varad on arvele võetud ja registrisse kantud.

10.1.2 P14S – Andmete säilitamise ja kõrvaldamise poliitika: tagab, et kasutuselt kõrvaldamiseks kavandatud süsteemid uuendatakse turvaliselt või nende andmed kustutatakse, vähendades kokkupuudet haavatavustega.

10.1.3 P17S – Andmekaitse ja privaatsuse poliitika: seab esikohale isikuandmeid töötlevate süsteemide haavatavuste kõrvaldamise, et täita andmekaitsealaseid õigusnõudeid.

10.1.4 P22S – Logimise ja seire poliitika: toetab paikamata süsteemide või kahtlase käitumise tuvastamist, mis võib viidata haavatavuse ärakasutamisele.

10.1.5 P30S – Intsidentidele reageerimise poliitika: määratleb protseduurid haavatavustele reageerimiseks, kui nende tagajärjel tekivad turbeintsidendid, sealhulgas eskaleerimise ja teavitamise sammud.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab kontrollimeetmete rakendamist tegevusriskide, sealhulgas haavatavuste halduse käsitlemiseks.

11.2 ISO/IEC 27002

11.2.1 Kontrollimeede 8.8 – määratleb protsessid süsteemides teadaolevate nõrkuste skannimiseks ja kõrvaldamiseks.

11.2.2 Kontrollimeede 8.9 – rõhutab turvalist konfiguratsiooni, paikade valideerimist ja muudatuste kontrolli, et vältida uuenduste käigus uute kokkupuutepunktide tekkimist.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – nõuab haavatavuste tuvastamist ja kõrvaldamist määratud tähtaegade jooksul.

11.3.2 SI-2 – nõuab paikade ja uuenduste viivitamatut rakendamist vastavalt nende kriitilisusele.

11.3.3 CM-2 – käsitleb süsteemi lähteseadistusi ja uuenduste dokumenteerimist, et tagada järjepidevad kaitsemeetmed.

11.4 EL GDPR

11.4.1 Artikkel 32(1)(b) – nõuab, et organisatsioonid rakendaksid asjakohaseid tehnilisi meetmeid, sealhulgas paikamist, et säilitada töötlemise turvalisus.

11.5 EL NIS2 direktiiv

11.5.1 Artikkel 21(2)(d) – nõuab haavatavuste käsitlemist süsteemse skannimise ja puuduste kõrvaldamise kaudu.

11.5.2 Artikkel 21(2)(e) – kohustab tagama turvalise konfiguratsiooni ja paikade halduse, et kindlustada IKT toimepidevus.

11.6 EL DORA

11.6.1 Artikkel 8(1) – nõuab IKT-riskide, sealhulgas tehniliste haavatavuste, tuvastamist ja maandamist.

11.6.2 Artikkel 10(2) – kohustab finantssektori üksusi kõrvaldama puudused, mis mõjutavad IKT-süsteeme ja tegevusi.

11.7 COBIT 2019

11.7.1 DSS05.02 – nõuab teadaolevate tehniliste haavatavuste käsitlemist turvaliste operatsioonide säilitamiseks.

11.7.2 APO12.01 – seob riskijuhtimise süsteemide nõrkuste ennetava seire ja parandamisega.