					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P18S					Dokumenta nosaukums: **Kriptogrāfisko kontroles pasākumu politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņotība ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	
ISO/IEC 27002:2022	Kontroles pasākumi 8.24, 8.25	
NIST SP 800-53 Rev. 5	SC-12 līdz SC-17	
ES NIS2	21. panta 2. punkta d) un e) apakšpunkts	
ES DORA	6. panta 2. punkta d) apakšpunkts, 9. panta 2. punkta f) apakšpunkts	
COBIT 2019	DSS05.01, APO13	
ES GDPR	32. panta 1. punkta a) apakšpunkts, 34. pants	

1. Mērķis

1.1 Šī politika nosaka obligātās prasības šifrēšanas un kriptogrāfisko kontroles pasākumu izmantošanai, lai aizsargātu komercdatu un personas datu konfidencialitāti, integritāti un autentiskumu.

1.2 Tā nodrošina kriptogrāfisko rīku atbilstošu izmantošanu sistēmās, iekārtās un mākoņpakalpojumos maza uzņēmuma vidē.

1.3 Šī politika tieši atbalsta ISO/IEC 27001:2022 sertifikāciju un palīdz organizācijai izpildīt Eiropas Savienības Vispārīgās datu aizsardzības regulas (GDPR), NIS2 direktīvas un Digitālās darbības noturības akta (DORA) prasības.

1.4 Šajā politikā aptvertie kriptogrāfiskie kontroles pasākumi ietver datu šifrēšanu, sertifikātu pārvaldību, drošu atslēgu pārvaldību un šifrētas rezerves kopijas.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem darbiniekiem, līgumslēdzējiem un trešajām personām, kas apstrādā uzņēmuma datus;

2.1.2 visām komercsistēmām, galiekārtām un mākoņplatformām, ko izmanto konfidenciālas informācijas glabāšanai, pārsūtīšanai vai piekļuvei tai;

2.1.3 visiem personas, finanšu, juridiskajiem vai sensitīvajiem ierakstiem, kas klasificēti saskaņā ar organizācijas Datu klasificēšanas un marķēšanas politiku;

2.1.4 visiem kriptogrāfiskajiem kontroles pasākumiem, tostarp šifrēšanas metodēm, atslēgām, parolēm, sertifikātiem un drošības moduļiem.

2.2 Politika aptver datus glabāšanā, datus pārsūtē un lietošanā esošus datus. Tā regulē arī šifrēšanu, ko izmanto rezerves kopijām, e-pastam, ārējai datu pārsūtīšanai un publiski pieejamām tīmekļvietnēm.

3. Mērķi

3.1 Nodrošināt, ka sensitīvi un regulēti dati vienmēr tiek aizsargāti ar atbilstošiem kriptogrāfiskiem pasākumiem.

3.2 Noteikt atbildību par šifrēšanas rīku izvēli, konfigurēšanu un atslēgu pārvaldību.

3.3 Novērst neatļautu piekļuvi, manipulācijas vai datu noplūdes, ieviešot drošus pārsūtīšanas un glabāšanas kontroles pasākumus.

3.4 Nodrošināt atbilstību tiesiskajām un regulatīvajām prasībām, kas paredz personas un komercdatu šifrēšanu.

3.5 Uzturēt darbības drošību un pieejamību, efektīvi pārvaldot sertifikātus un kriptogrāfiskās atslēgas.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 apstiprina šo politiku un nodrošina kriptogrāfisko prasību ieviešanu;

4.1.2 pārskata izņēmumus, paziņojumus par pārkāpumiem un piegādātāju atbilstību šifrēšanas prasībām;

4.1.3 pārliecinās, ka ārpakalpojumi un mākoņpakalpojumi atbilst šifrēšanas standartiem.

4.2 Ārējais IT pakalpojumu sniedzējs / iekšējais IT administrators

4.2.1 ievieš un uztur šifrēšanas risinājumus, piemēram, pilna diska šifrēšanu, SSL/TLS sertifikātus un VPN;

4.2.2 pārvalda kriptogrāfisko atslēgu dzīves ciklu un drošas glabāšanas risinājumus;

4.2.3 konfigurē un uzrauga šifrēšanu rezerves kopiju, tīmekļvietņu un iekārtu aizsardzībai.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējā pārskatīšana

9.1.1 Šī politika jāpārskata vismaz reizi gadā ģenerāldirektoram sadarbībā ar ārējo IT pakalpojumu sniedzēju un privātuma koordinatoru.

9.2 Starpposma pārskatīšanas ierosinātāji

9.2.1 Pārskatīšana jāveic arī, ja:

9.2.1.1 mainās kriptogrāfiskie standarti vai protokoli, piemēram, algoritma novecošanas dēļ;

9.2.1.2 tiek ieviestas jaunas sistēmas vai mākoņpakalpojumi;

9.2.1.3 pārkāpums vai incidents ir saistīts ar kompromitētu atslēgu vai sertifikātu;

9.2.1.4 tiesisko vai regulatīvo prasību izmaiņas ietekmē šifrēšanas prasības.

9.3 Versiju kontrole un saziņa

9.3.1 Visas politikas izmaiņas jādokumentē versiju kontroles žurnālā.

9.3.2 Personāls jāinformē par atjauninājumiem, un iepriekšējās versijas jāarhivē.

9.3.3 Jaunākā apstiprinātā versija jāglabā centrālajā politiku repozitorijā.

10. Saistītās politikas un sasaiste

10.1 Šī politika jāpiemēro kopā ar šādām SME politikām:

10.1.1 P12S – Aktīvu pārvaldības politika: nodrošina, ka šifrēšana tiek piemērota klasificētiem aktīviem glabāšanas, pārsūtīšanas un likvidēšanas laikā.

10.1.2 P14S – Datu glabāšanas politika un datu likvidēšanas prasības: nosaka glabāšanas termiņus un paredz datu šifrētu glabāšanu līdz to drošai dzēšanai.

10.1.3 P17S – Datu aizsardzības un privātuma politika: saskaņo šifrēšanu ar datu aizsardzības principiem un regulatīvajām prasībām saskaņā ar GDPR 32. pantu.

10.1.4 P22S – Žurnalēšanas un uzraudzības politika: nosaka atslēgu izmantošanas, šifrēšanas kļūmju un sertifikātu derīguma termiņu žurnalēšanu audita vajadzībām.

10.1.5 P30S – Incidentu pārvaldības politika: nosaka eskalācijas, ierobežošanas un paziņošanas procedūras gadījumiem, kad šifrēšana nedarbojas vai atslēgas ir kompromitētas.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts – nosaka darbības kontroles pasākumu, tostarp šifrēšanas, ieviešanu informācijas drošības risku pārvaldībai.

11.2 ISO/IEC 27002

11.2.1 8.24. kontroles pasākums – apraksta prasības šifrēšanas piemērošanai konfidencialitātes un integritātes nodrošināšanai.

11.2.2 8.25. kontroles pasākums – nosaka kriptogrāfisko atslēgu un sertifikātu drošas pārvaldības prasības.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – nosaka prasības kriptogrāfisko atslēgu izveidei un pārvaldībai.

11.3.2 SC-13 – nosaka prasības kriptogrāfiskās aizsardzības izmantošanai.

11.3.3 SC-17 – aptver publiskās atslēgas infrastruktūru (PKI) un sertifikātu dzīves cikla pārvaldību.

11.3.4 SC-28 – nosaka prasību šifrēt datus glabāšanā.

11.3.5 SC-12 līdz SC-17 kontroles saime – nodrošina, ka kriptogrāfiskie aizsardzības pasākumi ir pienācīgi ieviesti visās sistēmās.

11.4 ES GDPR

11.4.1 32. panta 1. punkta a) apakšpunkts – nosaka organizācijām pienākumu ieviest tehniskos pasākumus, piemēram, šifrēšanu, lai nodrošinātu datu konfidencialitāti.

11.4.2 34. pants – nosaka, ka šifrēšana var atbrīvot organizāciju no pienākuma paziņot par personas datu aizsardzības pārkāpumu, ja dati neatļautām personām bija nesaprotami.

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta d) apakšpunkts – nosaka efektīvas šifrēšanas izmantošanu sistēmu un sakaru aizsardzībai.

11.5.2 21. panta 2. punkta e) apakšpunkts – uzsver datu aizsardzību un kiberdraudu mazināšanu, izmantojot šifrēšanu.

11.6 ES DORA

11.6.1 6. panta 2. punkta d) apakšpunkts – nosaka, ka IKT sistēmām jāuztur droši sakaru kanāli un jānodrošina šifrēšana.

11.6.2 9. panta 2. punkta f) apakšpunkts – uzliek finanšu struktūrām pienākumu izmantot spēcīgu šifrēšanu digitālās saziņas un datu apmaiņas aizsardzībai.

11.7 COBIT 2019

11.7.1 DSS05.01 – nosaka sensitīvas informācijas aizsardzību, izmantojot šifrēšanu un kriptogrāfiskos protokolus.

11.7.2 APO13.02 – nosaka efektīvu drošības kontroles pasākumu ieviešanu, tostarp kriptogrāfiskos drošības pasākumus, kā daļu no informācijas drošības plānošanas.