					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P18					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**

Saskaņots ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	-
ISO/IEC 27002:2022	Kontroles pasākumi 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 līdz SC-17, SC-28, SC-28(1), SC-12(3)	-
EU GDPR	32. pants, 33.–34. pants, 83. apsvērums	-
EU NIS2	21. panta 2. punkta d) apakšpunkts	-
EU DORA	6. panta 2. punkta d) apakšpunkts, 11. panta 1. punkta c) apakšpunkts	-
COBIT 2019	DSS05.01, DSS06.06, MEA03	-

1. Mērķis

1.1 Šī politika nosaka obligātās prasības kriptogrāfisko kontroles pasākumu drošai un atbilstošai izmantošanai visā organizācijā, lai nodrošinātu sensitīvas un reglamentētas informācijas konfidencialitāti, integritāti un autentiskumu.

1.2 Kriptogrāfijas izmantošana ir būtiska datu drošības operāciju uzticamībai, atbalsta drošu saziņu, nodrošina piekļuves kontroli un sekmē normatīvo prasību izpildi, izmantojot efektīvu šifrēšanu un atslēgu pārvaldības praksi.

1.3 Šī politika ir saskaņota ar ISO/IEC 27001:2022 8. punktu un A pielikuma 8.24. kontroli, kā arī atbalsta juridisko un operacionālo pienākumu izpildi saskaņā ar GDPR 32. pantu, DORA 6. panta 2. punkta d) apakšpunktu un NIS2 21. pantu. Tā atbalsta arī COBIT 2019 mērķus attiecībā uz drošības pakalpojumiem un informācijas aktīvu aizsardzību.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām organizācijas struktūrvienībām, biznesa funkcijām, personālu un trešo pušu pakalpojumu sniedzējiem, kas ir iesaistīti kriptogrāfisko rīku un metožu izmantošanā, administrēšanā vai ieviešanā.

2.2 Aptvertās vides ietver ražošanas, izstrādes, testēšanas, rezerves kopēšanas un avārijas atjaunošanas sistēmas, kurās sensitīvi dati tiek pārsūtīti, apstrādāti vai glabāti.

2.3 Piemērošanas joma ietver visus kriptogrāfiskos komponentus un lietošanas gadījumus, tostarp, bet ne tikai:

2.3.1 Simetrisko un asimetrisko šifrēšanu

2.3.2 Digitālos parakstus un sertifikātus

2.3.3 Jaucējfunkciju algoritmus

2.3.4 Drošu atslēgu ģenerēšanu, izplatīšanu un iznīcināšanu

2.3.5 Transporta slāņa drošību (TLS), pilna diska šifrēšanu (FDE) un API līmeņa šifrēšanu

2.3.6 Drošus elementus, piemēram, aparatūras drošības moduļus (HSM), uzticamās platformas moduļus (TPM) un atslēgu pārvaldības sistēmas (KMS)

2.4 Šī politika regulē kriptogrāfijas izmantošanu attiecībā uz:

2.4.1 Datiem, kas klasificēti kā konfidenciāli, īpaši konfidenciāli vai reglamentēti

2.4.2 Autentifikāciju un digitālās identitātes pārbaudi

2.4.3 Drošu saziņu ar ārējām pusēm

2.4.4 Atslēgu glabāšanu un dubultās kontroles mehānismiem

3. Mērķi

3.1 Nodrošināt, ka kriptogrāfiskās tehnoloģijas tiek izvēlētas, apstiprinātas, ieviestas un uzturētas atbilstoši biznesa riskam, starptautiskajiem standartiem un normatīvajām prasībām.

3.2 Izveidot standartizētu pārvaldības struktūru kriptogrāfisko pakalpojumu pārvaldībai, tostarp skaidru atbildību par ieviešanu, validēšanu un izņēmumu pārvaldību.

3.3 Novērst kriptogrāfisko algoritmu un kontroles pasākumu neatļautu izmantošanu, nepareizu konfigurēšanu vai novecošanu, izmantojot formālu apstiprināšanas un pārskatīšanas procesu.

3.4 Nodrošināt, ka kriptogrāfiskie kontroles pasākumi tiek iestrādāti sistēmu projektēšanas posmā un regulāri validēti, lai novērstu datu izpaušanu, atslēgu kompromitēšanu vai protokolu degradāciju.

3.5 Nodrošināt visu kriptogrāfisko atslēgu dzīves cikla pārvaldību, tostarp ģenerēšanu, glabāšanu, izmantošanu, rotāciju, atsaukšanu un drošu iznīcināšanu.

3.6 Ievērot starptautiskās un reģionālās prasības, kas nosaka šifrēšanu un drošu datu apstrādi, tostarp GDPR, DORA, NIS2 un COBIT 2019.

4. Lomas un pienākumi

4.1 Informācijas drošības vadītājs / galvenais informācijas drošības vadītājs

4.1.1 Ir šīs politikas īpašnieks un nodrošina tās atbilstību IDPS un ISO/IEC 27001 A pielikuma 8.24. kontrolei.

4.1.2 Apstiprina kriptogrāfisko algoritmu un kontroles pasākumu izmantošanu un nodrošina atbilstību visā organizācijā.

4.2 Kriptogrāfisko operāciju vadītājs / drošības arhitekts

4.2.1 Pārvalda kriptogrāfisko sistēmu ikdienas darbību un administrēšanu.

4.2.2 Uztur apstiprināto kriptogrāfisko metožu sarakstu (ACML) un Atslēgu pārvaldības reģistru.

4.2.3 Veic kriptogrāfiskā dizaina pārskatīšanu (CDR) un izvērtē jaunas kriptogrāfiskās tehnoloģijas.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika katru gadu jāpārskata informācijas drošības vadītājam un Kriptogrāfisko operāciju vadītājam.

9.2 Pārskatīšanas ierosinātāji ietver:

9.2.1 kriptogrāfisko ievainojamību atklāšanu (piemēram, algoritmu pazemināšanas uzbrukumi, kvantu uzbrukumi)

9.2.2 normatīvo prasību izmaiņas, kuru dēļ nepieciešami atjaunināti šifrēšanas standarti

9.2.3 operatīvus vai audita konstatējumus, kas atklāj politikas trūkumus

9.2.4 kriptogrāfisko rīku atjauninājumus vai arhitektūras izmaiņas

9.3 Atjauninājumi jāpārvalda ar versiju kontroli IDPS dokumentu kontroles reģistrā un jāpaziņo:

9.3.1 visiem administratoriem ar kriptogrāfiskās piekļuves lomām

9.3.2 izstrādes komandām un DevSecOps vadītājiem

9.3.3 trešo pušu pakalpojumu sniedzējiem, uz kuriem attiecas līgumiskas šifrēšanas saistības

9.4 IDPS komandai jānodrošina, ka aizstātās versijas tiek arhivētas un uz tām vairs netiek atsaukts darbības procedūrās.

10. Saistītās politikas un sasaiste

10.1 P1 - Informācijas drošības politika. Tā nosaka pamatpārvaldību visiem drošības pasākumiem, tostarp kriptogrāfisko kontroles pasākumu piemērošanai, aktīvu aizsardzībai un drošai saziņai.

10.2 P4 - Piekļuves kontroles politika. Tā nodrošina, ka loģiskā piekļuve kriptogrāfiskajiem materiāliem un šifrēšanas pārvaldības sistēmām ir stingri ierobežota, pamatojoties uz minimālo privilēģiju principu un pienākumu nodalīšanu.

10.3 P6 - Risku pārvaldības politika. Tā atbalsta kriptogrāfisko kontroles pasākumu risku izvērtēšanu un dokumentē riska apstrādes stratēģiju izņēmumiem, algoritmu novecošanai vai atslēgu kompromitēšanas scenārijiem.

10.4 P12 - Aktīvu pārvaldības politika. Tā nosaka sensitīvu datu un aparatūras aktīvu klasificēšanu, kas tieši nosaka kriptogrāfiskās prasības un atslēgu glabāšanas pienākumus.

10.5 P13 - Datu klasificēšanas un marķēšanas politika. Tā definē klasifikācijas līmeņus (piemēram, konfidenciāli, reglamentēti), kas nosaka konkrētas šifrēšanas prasības pārsūtē un glabāšanā.

10.6 P14 - Datu glabāšanas un likvidēšanas politika. Tā nosaka procedūras šifrētu glabāšanas nesēju un kriptogrāfisko atslēgu materiāla drošai likvidēšanai dzīves cikla beigās.

10.7 P30 - Incidentu reaģēšanas politika. Tā nosaka organizācijas reaģēšanas stratēģiju atslēgu kompromitēšanas, sertifikātu neatbilstošas izmantošanas vai aizdomu par algoritmiskām ievainojamībām gadījumā, tostarp ātru atsaukšanu un ziņošanu par pārkāpumu.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts - Operacionālā plānošana un kontrole: nosaka tehnisko drošības kontroles pasākumu, tostarp kriptogrāfisko pasākumu, piemērošanu kā daļu no operacionālajiem aizsardzības pasākumiem.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroles pasākumi 8.24, 8.25, 8: sniedz ieviešanas vadlīnijas par kriptogrāfisko kontroles pasākumu mērķiem, algoritmu izvēli, protokolu piemērošanu un sertifikātu dzīves cikla pārvaldību.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 - Kriptogrāfisko atslēgu izveide: nosaka šifrēšanas atslēgu drošu ģenerēšanu un apmaiņu. P18 nosaka, kā simetriskās un asimetriskās atslēgas jāģenerē un jāapmaina, izmantojot apstiprinātus algoritmus un protokolus.

11.3.2 SC-13 - Kriptogrāfiskā aizsardzība: nosaka kriptogrāfijas izmantošanu informācijas konfidencialitātes un integritātes aizsardzībai. P18 nosaka šifrēšanu datiem glabāšanā un pārsūtē atbilstoši datu klasifikācijai, ar algoritmu standartiem, kas saskaņoti ar NIST FIPS 140-3.

11.3.3 SC-17 - Publiskās atslēgas infrastruktūras (PKI) sertifikāti: nosaka PKI ieviešanu autentifikācijas un digitālo parakstu atbalstam. P18 nosaka PKI izmantošanu saziņas, sistēmu identitāšu un administratīvās piekļuves aizsardzībai.

11.3.4 SC-28, SC-28(1) - Informācijas aizsardzība glabāšanā un pārsūtē: nosaka datu šifrēšanu, ja tie tiek glabāti vai pārsūtīti pa neuzticamiem tīkliem. P18 nosaka TLS, VPN tuneļu, pilna diska šifrēšanas un drošu glabāšanas metožu piemērošanu sensitīviem datiem.

11.3.5 SC-12(3) - Simetrisko atslēgu ģenerēšana drošai glabāšanai un izplatīšanai: koncentrējas uz simetrisko atslēgu drošu ģenerēšanu un apstrādi. P18 nosaka spēcīgu nejaušo skaitļu ģeneratoru izmantošanu, atslēgu rotācijas politiku un drošas atslēgu glabātuves kriptogrāfiskajām operācijām.

11.4 EU GDPR (2016/679)

11.4.1 32. pants - apstrādes drošība: tieši iesaka šifrēšanu kā personas datu riska samazināšanas pasākumu.

11.4.2 83. apsvērums: uzsver šifrēšanu kā kontroles pasākumu neatļautas piekļuves datiem novēršanai.

11.4.3 33. un 34. pants: efektīva šifrēšana var atbrīvot organizāciju no obligātās ziņošanas par pārkāpumu.

11.5 EU NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta d) apakšpunkts: nosaka tehniskus un organizatoriskus pasākumus, tostarp kriptogrāfisko aizsardzību, lai uzturētu pakalpojumu pieejamību un integritāti.

11.6 EU DORA (2022/2554)

11.6.1 6. panta 2. punkta d) apakšpunkts: finanšu iestādēm jāaizsargā dati, tostarp izmantojot stipru kritiskās informācijas šifrēšanu.

11.6.2 11. panta 1. punkta c) apakšpunkts: nosaka drošus datu apstrādes kontroles pasākumus IKT trešo pušu pakalpojumu sniedzējiem.

11.7 COBIT 2019

11.7.1 DSS05.01 - Informācijas aktīvu aizsardzība: nosaka šifrēšanas un atslēgu pārvaldības izmantošanu datu aizsardzībai pret neatļautu piekļuvi.

11.7.2 DSS06.06 - Pārvaldīta drošības testēšana: iesaka kriptogrāfiskās atbilstības validēšanu kā daļu no ievainojamību izvērtēšanas.

11.7.3 MEA03 - Atbilstības uzraudzība, izvērtēšana un novērtēšana: nosaka nepārtrauktu kriptogrāfisko kontroles pasākumu efektivitātes apliecināšanu.