

				Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P18				Teideal an doiciméid: Beartas um Rialuithe Cripteagrafacha							
Leagan: 1.0		Dáta teacht i bhfeidhm: 01.01.2025		Úinéir an doiciméid:							
X	Beartas		Caighdeán		Nós imeachta		Foirm		Clár		Eile

Stair na n-athbhreithnithe				
Uimhir na hathbhreithnithe	Dáta na hathbhreithnithe	Athruithe	Athbhreithnithe ag	Úinéir an phróisis

Formheasanna			
Ainm	Post	Dáta	Síniú

Fógra dlíthiúil (cóipcheart agus srianta úsáide)
(C) 2025 Clarysec LLC. All rights reserved.

Is maoin intleachtúil de chuid Clarysec LLC an doiciméad seo. Ní ceadmhach aon chuid den doiciméad seo a chóipeáil, a athúsáid, a dháileadh ná a mhodhnú chun críocha tráchtála ná cur chun feidhme gan cead sainráite i scríbhinn roimh ré.

Tá úsáid neamhúdaraíthe toirmiscithe go dian agus d'fhéadfadh caingean dlíthiúil a bheith mar thoradh uirthi. Le haghaidh ceadúnaithe, déan teagmháil le: info@clarysec.com

Ailínithe le caighdeáin agus rialacháin

Caighdeán/Rialachán	Clásal/Airteagal	Nóta
ISO/IEC 27001:2022	Clásal 8	-
ISO/IEC 27002:2022	Rialuithe 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12 go SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR an Aontais Eorpaigh	Airteagal 32, Airteagail 33–34, Aithris 83	-
NIS2 an Aontais Eorpaigh	Airteagal 21(2)(d)	-
DORA an Aontais Eorpaigh	Airteagail 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Cuspóir

1.1 Sainmhínítear sa bheartas seo na ceanglais éigeantacha maidir le húsáid shlán agus chomhlíontach rialuithe cripteagrafacha ar fud na heagraíochta chun rúndacht, sláine agus barántúlacht faisnéise íogaire agus rialáilte a chinntiú.

1.2 Tacaíonn úsáid na cripteagrafaíochta le hiontaoibh in oibríochtaí slándála sonraí, le cumarsáid shlán, le cur chun feidhme rialaithe rochtana, agus le comhlíonadh rialála trí chleachtais éifeachtacha criptiúcháin agus bainistíochta eochracha.

1.3 Tá an beartas seo ailínithe le Clásal 8.1 de ISO/IEC 27001:2022 agus le Rialú 8.24 d'larscríbhinn A, agus tacaíonn sé le hoibleagáidí dlíthiúla agus oibríochtúla faoi Airteagal 32 den GDPR, Airteagal 6(2)(d) de DORA, agus Airteagal 21 de NIS2. Tacaíonn sé freisin le cuspóirí COBIT 2019 maidir le seirbhísí slándála agus cosaint sócmhainní sonraí.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir le gach aonad eagraíochtúil, feidhm ghnó, ball foirne agus soláthraí seirbhíse tríú páirtí a bhfuil baint acu le húsáid, riaradh nó cur chun feidhme uirlisí agus modhanna cripteagrafacha.

2.2 Áirítear leis sin timpeallachtaí táirgthe, forbartha, stáitsithe, cúltaca agus athshlánaithe ó thubaiste ina ndéantar sonraí íogaire a tharchur, a phróiseáil nó a stóráil.

2.3 Áirítear sa raon feidhme gach comhpháirt agus cás úsáide cripteagrafach, lena n-áirítear, ach gan a bheith teoranta do:

2.3.1 Criptiú siméadrach agus neamhshiméadrach

2.3.2 Sínithe digiteacha agus teastais dhigiteacha

2.3.3 Algartaim haisceála

2.3.4 Giniúint, dáileadh agus scriosadh slán eochracha

2.3.5 Slándáil Sraithe Iompair (TLS), criptiú diosca iomláin (FDE), agus criptiú ar leibhéal API

2.3.6 Eilimintí slána amhail Modúil Slándála Crua-earraí (HSManna), Modúil Ardáin Iontaofa (TPManna), agus Córais Bainistíochta Eochracha (KMS)

2.4 Rialaítear leis an mbeartas seo úsáid na cripteagrafaíochta i ndáil le:

2.4.1 Sonraí aicmithe mar Rúnda, An-Rúnda, nó Rialáilte

2.4.2 Fíordheimhniú agus fóruí aitheantais dhigitigh

2.4.3 Cumarsáid shlán le páirtithe seachtracha

2.4.4 Coimeád eochracha agus sásraí dé-rialaithe

3. Cuspóirí

3.1 A chinntiú go roghnaítear, go bhformheastar, go gcuirtear chun feidhme agus go gcothaítear teicneolaíochtaí cripteagrafacha i gcomhréir le riosca gnó, caighdeáin idirnáisiúnta agus sainorduithe rialála.

3.2 Struchtúr rialachais caighdeánaithe a bhunú chun seirbhísí cripteagrafacha a bhainistiú, lena n-áirítear cuntasacht shoiléir as cur chun feidhme, bailíochtú agus láimhseáil eisceachtaí.

3.3 Cosc a chur ar úsáid neamhúdaraíthe, ar mhíchumraíocht, nó ar dhul in éag algartam agus rialuithe cripteagrafacha trí phróiseas foirmiúil formheasa agus athbhreithnithe.

3.4 A chinntiú go mbíonn rialuithe cripteagrafacha leabaithe i gcéim dheartha an chórais agus go mbailíochtaítear go rialta iad chun nochtadh sonraí, comhréiteach eochracha, nó díghrádú prótacal a chosc.

3.5 Bainistíocht shaolré gach eochrach cripteagrafach a chur chun feidhme, lena n-áirítear giniúint, stóráil, úsáid, rothlú, cúlghairm agus scriosadh slán.

3.6 Comhlíonadh a chinntiú le rialacháin idirnáisiúnta agus réigiúnacha a éilíonn criptiú agus láimhseáil shlán sonraí, lena n-áirítear GDPR, DORA, NIS2 agus COBIT 2019.

4. Ról agus freagrachtaí

4.1 Bainisteoir Slándála Faisnéise / Príomhoifigeach Slándála Faisnéise (CISO)

4.1.1 Is leis an ról seo an beartas seo agus cinntíonn sé ailíniú leis an gCóras Bainistíochta Slándála Faisnéise (ISMS) agus le Rialú 8.24 d'Iarscríbhinn A de ISO/IEC 27001.

4.1.2 Formheasann sé úsáid algartam agus rialuithe cripteagrafacha agus cinntíonn sé comhlíonadh ar fud na heagraíochta.

4.2 Ceannaire Oibríochtaí Cripteagrafacha / Ailtire Slándála

4.2.1 Bainistíonn sé oibríochtaí agus riarachán laethúil na gcóras cripteagrafach.

4.2.2 Coinníonn sé Liosta na Modhanna Cripteagrafacha Ceadaithe (ACML) agus an Clár Bainistíochta Eochracha.

4.2.3 Déanann sé Athbhreithnithe Dearaidh Cripteagrafacha (CDRanna) agus measúnaíonn sé teicneolaíochtaí cripteagrafacha nua.

[... Níl ailt 4.3–8 san áireamh sa réamhamharc seo. Ceannaigh an doiciméad iomlán chun rochtain a fháil ar an gcomhábhar iomlán. ...]

9. Ceanglais athbhreithnithe agus nuashonraithe

9.1 Déanfaidh an Bainisteoir Slándála Faisnéise agus an Ceannaire Oibríochtaí Cripteagrafacha athbhreithniú bliantúil ar an mbeartas seo.

9.2 Áirítear na nithe seo a leanas mar spreagthaí athbhreithnithe:

9.2.1 Leochaileachtaí cripteagrafacha a aimsiú (m.sh. íslíú algartam, ionsaithe chandamacha)

9.2.2 Athruithe rialála a éilíonn caighdeáin chriptiúcháin nuashonraithe

9.2.3 Torthaí oibríochtúla nó iniúchta a nochtann bearnaí sa bheartas

9.2.4 Uasghráduithe ar uirlisí cripteagrafacha nó athruithe ailtireachta

9.3 Ní mór nuashonruithe a bheith faoi rialú leaganacha i gClár Rialaithe Doiciméad an ISMS agus iad a chur in iúl do:

9.3.1 Gach riarthóir a bhfuil ról rochtana cripteagrafacha acu

9.3.2 Foirme forbartha agus ceannairí DevSecOps

9.3.3 Soláthraithe tríú páirtí atá faoi oibleagáidí conarthacha criptiúcháin

9.4 Ní mór d'fhoireann an ISMS a chinntiú go ndéantar leaganacha atá curtha as feidhm a chartlannú agus nach ndéantar tagairt dóibh a thuilleadh i nósanna imeachta oibriúcháin.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 P1 - Beartas Slándála Faisnéise. Soláthraíonn sé an bonn rialachais do gach beart slándála, lena n-áirítear cur chun feidhme rialuithe cripteagrafacha, cosaint sócmhainní agus cumarsáid shlán.

10.2 P4 - Beartas Rialaithe Rochtana. Cinntíonn sé go bhfuil rochtain loighciúil ar ábhar cripteagrafach agus ar chórais bhainistíochta criptiúcháin teoranta go dian ar bhonn phrionsabal na pribhléide íosta agus scaradh dualgas.

10.3 P6 - Beartas Bainistíochta Riosca. Tacaíonn sé le measúnú rioscaí a bhaineann le rialuithe cripteagrafacha agus doiciméadaíonn sé an straitéis cóireála riosca le haghaidh eisceachtaí, dul in éag algartam, nó cásanna comhréitigh eochracha.

10.4 P12 - Beartas Bainistíochta Sócmhainní. Éilíonn sé aicmiú sonraí íogaire agus sócmhainní crua-earraí, rud a chinneann go díreach na ceanglais chripteagrafacha agus oibleagáidí coimeáda eochracha.

10.5 P13 - Beartas Aicmithe agus Lipéadaithe Sonraí. Sainmhíníonn sé na leibhéil aicmithe (m.sh. Rúnda, Rialáilte) a spreagann ceanglais shonracha criptiúcháin faoi bhealach agus ar fos.

10.6 P14 - Beartas um Choinneáil agus Diúscairt Sonraí. Sonraíonn sé nósanna imeachta maidir le diúscairt shlán meán stórála criptithe agus ábhair eochrach cripteagrafach ag deireadh a saoil.

10.7 P30 - Beartas um Fhreagairt do Theagmhais. Leagtar amach ann straitéis freagartha na heagraíochta i gcás comhréiteach eochracha, mí-úsáid teastais, nó leochaileachtaí algartamacha amhrasta, lena n-áirítear cúlghairm thapa agus tuairisciú sáraithe.

11. Caihdeáin agus creatáil tagartha

11.1 ISO/IEC 27001

11.1.1 Clásal 8.1 - Pleanáil agus Rialú Oibríochtúil: Cuirtear rialuithe slándála teicniúla, lena n-áirítear bearta cripteagrafacha, chun feidhme mar chuid de na coimircí oibríochtúla.

11.2 ISO/IEC 27002:2022

11.2.1 Rialuithe 8.24, 8.25, 8: Soláthraítear treoir maidir le cur chun feidhme cuspóirí rialaithe cripteagrafacha, roghnú algartam, cur chun feidhme prótacal, agus bainistíocht shaolré teastais.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Bunú Eochrach Chripteagrafach: Cinntítear giniúint agus malartú slán eochracha criptiúcháin. Sainítear in P18 conas is gá eochracha siméadracha agus neamhshiméadracha a ghiniúint agus a mhalartú trí úsáid a bhaint as algartaim agus prótacail cheadaithe.

11.3.2 SC-13 - Cosaint Chripteagrafach: Éilítear úsáid na cripteagrafaíochta chun rúndacht agus sláine faisnéise a chosaint. Cuireann P18 criptiú ar fos agus faoi bhealach chun feidhme bunaithe ar aicmiú sonraí, le caighdeáin algartam ailínithe le NIST FIPS 140-3.

11.3.3 SC-17 - Teastais Bonneagair Eochrach Phoiblí (PKI): Éilítear PKI a chur chun feidhme chun tacú le fíordheimhniú agus le sínithe digiteacha. Leagtar amach in P18 úsáid PKI chun cumarsáid, aitheantais chórais agus rochtain riaracháin a dhaingniú.

11.3.4 SC-28, SC-28(1) - Cosaint Faisnéise ar Fos agus Faoi Bhealach: Éilítear criptiú sonraí nuair a stóráiltear iad nó nuair a tharchuirtear iad thar líonraí neamhiontaofa. Sonraítear in P18 cur chun feidhme TLS, tolláin VPN, criptiú diosca iomláin agus modhanna stórála slána le haghaidh sonraí íogaire.

11.3.5 SC-12(3) - Giniúint Eochrach Siméadrí le haghaidh Stóráil agus Dáileadh Slán: Dírítear ar eochracha siméadracha a ghiniúint agus a láimhseáil go slán. Éilíonn P18 úsáid gineadóirí láidre

uimhreacha randamacha, beartais rothlaithe eochracha agus bogtaí slána eochracha le haghaidh oibríochtaí cripteagrafacha.

11.4 GDPR an Aontais Eorpaigh (2016/679)

11.4.1 Airteagal 32 - Slándáil na Próiseála: Moltar criptiú go sainráite mar bheart chun riosca a laghdú i leith sonraí pearsanta.

11.4.2 Aithris 83: Leagtar béim ann ar chriptiú mar rialú chun rochtain neamhúdaraithe ar shonraí a chosc.

11.4.3 Airteagail 33 agus 34: Féadfaidh criptiú eagraíochtaí a dhíolmhú ó fhógraí éigeantacha sáraithe má tá sé éifeachtach.

11.5 Treoir NIS2 an Aontais Eorpaigh (2022/2555)

11.5.1 Airteagal 21(2)(d): Éilítear bearta teicniúla agus eagraíochtúla, lena n-áirítear cosaintí cripteagrafacha, chun infhaighteacht agus sláine seirbhíse a chothabháil.

11.6 DORA an Aontais Eorpaigh (2022/2554)

11.6.1 Airteagal 6(2)(d): Ní mór d'institiúidí airgeadais sonraí a dhaingniú, lena n-áirítear trí chriptiú láidir ar fhaisnéis chriticiúil.

11.6.2 Airteagal 11(1)(c): Éilítear rialuithe slána próiseála sonraí ar sholáthraithe seirbhíse TFC tríú páirtí.

11.7 COBIT 2019

11.7.1 DSS05.01 - Sócmhainní Faisnéise a Chosaint: Éilítear úsáid criptiúcháin agus bainistíochta eochracha chun sonraí a chosaint ar rochtain neamhúdaraithe.

11.7.2 DSS06.06 - Tástáil Shlándála Bhainistithe: Moltar bailíochtú comhlíonta cripteagrafach mar chuid de mheasúnuithe leochaileachta.

11.7.3 MEA03 - Faireachán, Meastóireacht agus Measúnú ar Chomhlíonadh: Cuirtear dearbhú leanúnach chun feidhme maidir le héifeachtacht rialuithe cripteagrafacha.