

				Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P02				Teideal an doiciméid: Beartas um Róil agus Freagrachtaí Rialachais							
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

Ailíniú le caighdeáin agus rialacháin

Caighdeán/Rialachán	Clásal/Airteagal	Nóta
ISO/IEC 27001:2022	Clásal 5.3; Rialú 5 d'Iarscríbhinn A	
ISO/IEC 27002:2022	Rialú 5	
NIST SP 800-53 Rev.5	PL-1 go PL-4, PM-1 go PM-13	
RGCS an Aontais Eorpaigh	Airteagail 5(1)(f), 24, 37	
Treoir NIS2 an Aontais Eorpaigh	Airteagal 21(2)(a)	
Rialachán DORA an Aontais Eorpaigh	Airteagal 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Cuspóir

1.1 Sainmhínítear sa bheartas seo an tsamhail rialachais, na ról eagraíochtúla agus na freagrachtaí is gá chun Córas Bainistíochta Slándála Faisnéise (ISMS) éifeachtach a oibriú.

1.2 Bunaítear leis línte soiléire cuntasachta, údarás cinnteoireachta agus conairí uaschéimnithe chun a chinntiú go bhfuil slándáil faisnéise leabaithe ag gach leibhéal den eagraíocht agus ailínithe le cuspóirí straitéiseacha gnó.

1.3 Tacaíonn an beartas seo le ceanglais ISO/IEC 27001:2022, Clásal 5.3, agus Rialú A.5.2, agus cinntíonn sé go sannfar, go ndoiciméadófar, go gcuirfear in iúl agus go n-athbhreithneofar go tréimhsiúil freagrachtaí do ghníomhaíochtaí a bhaineann le slándáil.

1.4 Soláthraíonn an beartas seo bunús freisin do rialachas comhtháite le disciplíní eile, amhail bainistíocht riosca, comhlíonadh, oibríochtaí TF agus feidhmeanna dlí.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir le gach duine agus eintiteas a bhfuil baint acu le rialachas, oibriú agus maoirseacht na slándála faisnéise laistigh de raon feidhme an ISMS. Áirítear leis seo:

2.1.1 An cheannaireacht fheidhmiúcháin, an bhainistíocht shinsearach agus comhaltaí an bhoird

2.1.2 Bainisteoirí ISMS, CISOanna agus úinéirí rialuithe

2.1.3 Úinéirí próisis agus úinéirí sócmhainní

2.1.4 Conraitheoirí agus soláthraithe seirbhíse tríú páirtí a bhfuil freagrachtaí slándála tarmligthe dóibh

2.2 Clúdaítear leis feidhmeanna inmheánacha agus seachfhoinsithe araon (e.g. SOC seachfhoinsithe, riarthóirí ardáin scamallbhunaithe) nuair a shanntar ról rialachais go foirmiúil nó nuair a shainmhínítear iad go conarthach.

2.3 Tá feidhm ag an mbeartas seo freisin maidir le haonaid eagraíochtúla, ranna agus foirne tionscadail a bhainistíonn nó a imríonn tionchar ar shócmhainní, córais nó seirbhísí atá ábhartha don tsándáil.

3. Cuspóirí

3.1 A chinntiú go sainmhínítear, go sannfar, go gcuirfear in iúl agus go ndoiciméadófar ról agus freagrachtaí slándála faisnéise go foirmiúil.

3.2 Samhail rialachais a chothabháil a chuireann scaradh dualgas i bhfeidhm, a sheachnaíonn coinbhleachtaí leasa, agus a chumasaíonn uaschéimniú ar shaincheisteanna slándála gan réiteach.

3.3 A chinntiú go leithdháiltear cuntasacht agus údarás do chinntí slándála de réir tionchair ghnó agus struchtúir eagraíochtúla.

3.4 Creat a bhunú chun tarmligeán, athruithe ról agus athbhreithniú ar fhreagrachtaí sannta a bhainistiú.

3.5 Dearbhú rialaithe a sholáthar do pháirtithe leasmhara, lena n-áirítear rialtóirí, iniúcháirí agus cliaint, go bhfuil slándáil faisnéise á rialú go héifeachtach agus de réir na gcaighdeán infheidhme.

4. Róil agus freagrachtaí

4.1 An Bhainistíocht Fheidhmiúcháin (an Ardbhainistíocht)

4.1.1 Soláthraíonn sí maoirseacht straitéiseach, leithdháileann sí acmhainní agus cinntíonn sí ailíniú idir cuspóirí an ISMS agus spriocanna gnó.

4.1.2 Faomhann sí príomhdhoiciméadú an ISMS, lena n-áirítear an Beartas Slándála Faisnéise, pleananna cóireála agus cinntí maidir le hullmhacht iniúchta.

4.1.3 Glacann sí páirt in athbhreithnithe bainistíochta an ISMS agus déanann sí cinntí a dteastaíonn faomhadh ar leibhéal an bhoird ina leith a uaschéimniú.

4.1.4 Tacaíonn sí le cultúr slándála agus cuireann sí comhlíonadh na heagraíochta le prionsabail rialachais slándála chun cinn.

4.2 An Coiste Stiúrtha Slándála Faisnéise (ISSC)

4.2.1 Feidhmíonn sé mar an comhlacht rialachais trasfheidhmeach do mhaoirseacht an ISMS.

4.2.2 Déanann sé athbhreithniú ar stádas riosca, ar fheidhmíocht rialuithe, ar fhionnachtana iniúchta agus ar thionscnaimh straitéiseacha slándála.

4.2.3 Éascaíonn sé comhordú idir ranna (e.g. TF, dlí, AD, riosca, comhlíonadh, oibríochtaí).

4.2.4 Faomhann sé tairseacha uaschéimnithe, leithdháiltí buiséid agus athruithe beartais a éilíonn ionchur feidhmiúcháin.

[... 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 Sceideal athbhreithnithe

9.1.1 Déanfar athbhreithniú ar an mbeartas seo uair sa bhliain ar a laghad nó nuair a tharlóidh aon cheann díobh seo a leanas:

9.1.1.1 Athruithe ar an struchtúr eagraíochtúil nó ar an bhfoireann feidhmiúcháin

9.1.1.2 Leathnú nó athshainmhíniú ar raon feidhme an ISMS

9.1.1.3 Athruithe rialála a dhéanann difear do shannadh ról nó do mhaoirseacht

9.1.1.4 Fionnachtana iniúchta suntasacha nó teagmhais a bhaineann le teip rialachais

9.2 Próiseas athbhreithnithe agus formheasa

9.2.1 Déanfaidh an Bainisteoir ISMS an próiseas athbhreithnithe a thionscnamh agus a stiúradh, lena n-áirítear bailiú ionchuir ó pháirtithe leasmhara agus aiseolais iniúchta.

9.2.2 Déanfaidh an ISSC athbhreithniú ar nuashonruithe beartaithe agus déanfaidh an Bhainistíocht Fheidhmiúcháin iad a fhaomhadh go foirmiúil.

9.2.3 Ní mór gach leagan a rianú i gClár Doiciméad an ISMS agus ní mór na meiteashonraí seo a leanas a bheith san áireamh ann:

9.2.3.1 Aitheantas agus teideal an bheartais

9.2.3.2 Uimhir an leagain agus achoimre ar na hathruithe

9.2.3.3 Dáta éifeachta agus dáta an chéad athbhreithnithe eile

9.2.3.4 Úinéir agus faomhthóir an bheartais

9.2.3.5 Leibhéal aicmithe an doiciméid

9.2.3.6 Stair coinneála agus chartlannaithe

10. Beartais ghaolmhara agus naisc eatarthu

10.1 Ba cheart an beartas seo a léirmhíniú i gcomhar leis na beartais seo a leanas:

10.1.1 P1 – Beartas Slándála Faisnéise: Bunaítear leis an clár slándála foriomlán agus leagtar amach ann freagrachtaí ceannaireachta maidir le formhuiniú beartais agus maoirseacht straitéiseach.

10.1.2 P5 – Beartas um Bainistíocht Athruithe: Cinntíonn sé go bhfuil athruithe ar struchtúir rialachais, ról nó freagrachtaí faoi réir formheasa doiciméadaithe agus athbhreithnithe riosca.

10.1.3 P6 – Beartas Bainistíochta Riosca: Aithníonn sé agus cóireálann sé rioscaí rialachais a eascraíonn as coinbhleachtaí ról, dualgais neamshannta nó easpa uaschéimnithe.

10.1.4 P7 – Beartas um Ionduchtú agus Foirceannadh: Cuireann sé próisis sannacháin agus aisghairme rialuithe i bhfeidhm le linn athruithe i saolré pearsanra.

10.1.5 P33 – Beartas um Fhaireachán Iniúchta agus Comhlíonta: Tacaíonn sé le hathbhreithniú neamhspleách ar éifeachtacht rialachais agus cuireann sé gníomhartha ceartaitheacha i bhfeidhm le haghaidh neamhchomhlíonta.

10.2 Tacaíonn na beartais seo le chéile le creat rialachais aontaithe agus infhorfheidhmithe don ISMS.

11. Caighdeáin agus creataí tagartha

11.1 Tá an beartas seo ailínithe le caighdeáin agus creataí a aithnítear go hidirnáisiúnta maidir le rialachas slándála faisnéise agus cuntasacht ról. Cinntíonn sé inrianaitheacht chuig ceanglais rialála agus deimhniúcháin, agus tacaíonn sé le struchtúr ISMS atá inchosanta.

11.2 ISO/IEC 27001

11.2.1 Clásal 5.3 – Róil, Freagrachtaí agus Údaráis Eagraíochtúla: Comhlíonann an beartas seo an ceanglas go sannfar, go gcuirfear in iúl agus go ndoiciméadófar go soiléir róil a bhaineann le slándáil faisnéise.

11.2.2 Clásal 9.3 – Athbhreithniú bainistíochta: Cuireann an beartas seo maoirseacht fheidhmiúcháin ar róil agus ar rialachas an ISMS i bhfeidhm trí athbhreithnithe ráithiúla agus bliantúla.

11.2.3 Rialú 5.2 d'Iarscríbhinn A – Róil agus Freagrachtaí Slándála Faisnéise: Sainmhínítear leis róil ar fud leibhéal theicniúla, oibríochtúla agus straitéiseacha chun scaradh dualgas, úinéireacht riosca agus cuntasacht inrianaithe a chinntiú.

11.3 ISO/IEC 27002:2022 – Rialú 5

11.3.1 Soláthraíonn sé treoir chur chun feidhme maidir le freagrachtaí slándála faisnéise a shannadh ar fud na heagraíochta. Glacann an beartas seo leis an treoir sin trí chineálacha ról, rialacha tarmiligthe, nósanna imeachta uaschéimnithe agus sásraí athbhreithnithe a shainiú.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 go PL-4: Leagtar amach leo an gá atá le doiciméadú foirmiúil pleanála, lena n-áirítear beartais a shainíonn rialachas agus a shannann freagrachtaí slándála.

11.4.2 PM-1 (Plean Chláir Slándála Faisnéise) agus PM-2 (Príomhoifigeach Slándála Faisnéise): Léirítear iad sa bheartas seo trí shannadh an CISO/Bhainisteora ISMS agus róil fhoirmiúla rialachais.

11.4.3 PM-5 go PM-13: Comhlíonann an beartas seo ceanglais maidir le doiciméadú ról, ról riosca ar fud na heagraíochta, maoirseacht ar bhainistíocht cumraíochta agus comhtháthú le feidhmeanna misean/gnó.

11.5 RGCS an Aontais Eorpaigh (2016/679)

11.5.1 Airteagal 5(1)(f): Ceanglaíonn sé sonraí pearsanta a chosaint ar phróiseáil neamhúdaráithe nó neamhdhleathach. Cinntíonn an beartas seo go n-ainmnítear go soiléir agus go ndéantar faireachán ar dhaoine aonair atá freagrach as cosaint sonraí.

11.5.2 Airteagal 24: Ceanglaíonn sé bearta eagraíochtúla iomchuí, lena n-áirítear struchtúir rialachais.

11.5.3 Airteagal 37: Ceanglaíonn sé Oifigeach Cosanta Sonraí (DPO) a ainmniú, agus ní mór é sin a léiriú i gcreat rialachais agus i gclár freagrachtaí na heagraíochta.

11.6 Treoir NIS2 an Aontais Eorpaigh (2022/2555)

11.6.1 Airteagal 21(2)(a): Forordaítear leis go gcuireann eintitis beartais i bhfeidhm maidir le hanailís riosca agus slándáil córas faisnéise, lena n-áirítear freagrachtaí rólshonracha. Sainmhínítear sa bheartas seo ról den sórt sin agus a sásraí rialachais.

11.7 Rialachán DORA an Aontais Eorpaigh (2022/2554)

11.7.1 Airteagal 5 – Creat Rialachais agus Rialaithe Inmheánaigh: Ceanglaíonn sé sannadh foirmiúil freagrachtaí bainistíochta riosca TFC, ról cinnteoireachta agus bealaí tuairiscithe. Soláthraíonn an beartas seo an bonn do rialachas ról a bhaineann le slándáil i dtimpeallachtaí TFC.

11.8 COBIT 2019

11.8.1 EDM01 – Ensured Governance Framework Setting: Cinntíonn an beartas seo go bhfuil struchtúr rialachais sainithe go soiléir ag an ISMS agus go bhfuil sé ailínithe le riachtanais na heagraíochta.

11.8.2 EDM02 – Ensured Benefits Delivery: Ailíníonn sé gníomhaíochtaí slándála rólhunaithe le cuspóirí straitéiseacha agus oibríochtúla, agus cinntíonn sé cuntasacht agus torthaí intomhaiste.

11.8.3 APO01 – Managed I&T Management Framework agus APO12 – Managed Risk: Tacaíonn an beartas seo le bainistiú struchtúrtha ar ról slándála faisnéise laistigh de chreat níos leithne rialachais agus riosca TF.

11.8.4 MEA01 – Monitor, Evaluate and Assess Performance: Leabhaíonn sé sásraí athbhreithnithe chun a fhíorú go bhfuil ról rialachais éifeachtach, cothrom le dáta agus curtha chun feidhme.