

				Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P01S				Teideal an doiciméid: Beartas Slándála Faisnéise							
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 neamhúdaráithe toirmiscthe 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	Clásail 5.1, 5.2, 5.3, 6.1, 6.2, 8	Sonraítear tiomantas na bainistíochta, ceanglais bheartais, sannadh rólanna, measúnú riosca agus rialú oibríochtúil
ISO/IEC 27002:2022	Rialuithe 5.1–5	Sonraítear beartas slándála faisnéise doiciméadaithe a bhunú, sannadh rólanna, scaradh dualgas agus freagrachtaí bainistíochta
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Ceanglais maidir le plean slándála faisnéise, beartas pleanála, measúnú/údarú agus rialú rochtana
GDPR an Aontais Eorpaigh (2016/679)	Airteagal 5(2), Airteagal 32	Prionsabal na cuntasachta agus bearta maidir le slándáil próiseála, go háirithe i ndáil le rólanna doiciméadaithe
Treoir NIS2 an Aontais Eorpaigh (2022/2555)	Airteagal 21(2)(a)	Ceanglaítear bearta bainistíochta riosca, rólanna agus freagrachtaí maidir le cibearriosca
DORA an Aontais Eorpaigh (2022/2554)	Airteagal 9, Airteagal 10	Ceanglaítear sannadh rólanna maidir le bainistíocht riosca TFC agus leanúnachas gnó
COBIT 2019	EDM03, APO13, DSS05	Cinntítear barrfheabhsú riosca, bainistíocht slándála agus bainistíocht seirbhísí slándála trí shannadh soiléir rólanna

1. Cuspóir

1.1 Léiríonn an beartas seo tiomantas na heagraíochta do chosaint faisnéise custaiméirí agus faisnéise gnó trí fhreagrachtaí soiléire agus bearta praiticiúla slándála a shainiú, atá oiriúnach d'eagraíochtaí nach bhfuil foirne tiomnaithe TF acu.

1.2 Cinntíonn sé go gcloíonn gach fostaí, conraitheoir agus soláthraí seirbhíse le rialacha infhorfheidhmithe, rud a chumasaíonn comhlíonadh iomlán cheanglais deimhniúcháin ISO/IEC 27001.

1.3 Cumasaíonn an beartas seo don eagraíocht muinín custaiméirí a chothú trí léiriú soiléir a thabhairt ar an gcaoi a gcosnaítear a gcuid faisnéise trí fhreagrachtaí sainithe, próisis struchtúrtha agus cuntasacht láidir.

2. Raon feidhme

2.1 Baineann an beartas seo le gach duine a fhaigheann rochtain ar shonraí agus ar chórais na heagraíochta nó a bhainistíonn iad, lena n-áirítear:

2.1.1 Úinéirí gnó agus bainisteoirí ginearálta

2.1.2 Fostaithe, conraitheoirí agus intéirínigh

2.1.3 Soláthraithe seachtracha seirbhísí TF nó comhairleoirí

2.2 Cumhdaítear leis gach cineál faisnéise, córas agus seirbhíse, lena n-áirítear:

2.2.1 Taifid ghnó, sonraí custaiméirí, pasfhocail agus ríomhphoist

2.2.2 Crua-earraí TF amhail ríomhairí glúine agus fóin

2.2.3 Seirbhísí néalríomhaireachta a úsáidtear chun comhaid a stóráil, le haghaidh cumarsáide nó airgeadais

2.2.4 Doiciméid fhisiciúla a stóráiltear in áitribh oifige

2.3 Tá feidhm ag an mbeartas seo i ngach timpeallacht oibre — san oifig, go cianda agus sa néal — agus áirítear leis gach gléas agus bogearra a úsáidtear chun faisnéis ghnó a phróiseáil nó a stóráil.

3. Cuspóirí

3.1 Freagracht shoiléir a shannadh: A chinntiú go mbíonn duine freagrach i gcónaí as slándáil faisnéise. De ghnáth is é seo an Bainisteoir Ginearálta nó an duine a ainmníonn sé/sí go foirmiúil.

3.2 Faisnéis custaiméirí agus faisnéis ghnó a chosaint: Coimircí iontaofa comhsheasmhacha a chur i bhfeidhm chun mí-úsáid, cailteanas nó goid sonraí íogaire a chosc, lena n-áirítear taifid chustaiméirí agus taifid airgeadais.

3.3 Tacú le deimhniú ISO/IEC 27001: A chumasú don eagraíocht comhlíonadh iomlán cheanglais ISO/IEC 27001 a léiriú, chun ullmhacht iniúchta agus incháilitheacht deimhniúcháin a áirithiú gan bonneagar casta a bheith ag teastáil.

3.4 Slándáil a leabú in oibríochtaí gnó: Slándáil faisnéise a chomhtháthú i dtascanna agus i gcintí laethúla ar fud na heagraíochta.

3.5 Feasacht agus cultúr slándála a chothú: Gach fostaí a spreagadh chun cleachtais slándála a thuiscint agus a chothabháil, amhail pasfhocail láidre a úsáid agus gníomhaíocht amhrasach a thuirisciú.

4. Rólanna agus Freagrachtaí

4.1 Bainisteoir Ginearálta nó Úinéir an Ghnó

4.1.1 Tá cuntasacht fhoriomlán air/uirthi as slándáil faisnéise.

4.1.2 Formheasann sé/sí an beartas seo agus cinntíonn sé/sí go gcoimeádtar cothrom le dáta é.

4.1.3 Cinntíonn sé/sí go ndéantar na príomhthascanna slándála uile a bhainistiú go díreach nó a tharmligean i scríbhinn.

4.1.4 Fíoraíonn sé/sí go gcuirtear i gcrích go héifeachtach aon tascanna slándála a tharmligear, amhail bainistíocht rochtana nó freagairt do theagmhais.

4.1.5 Feidhmíonn sé/sí mar phríomhtheagmhálaí réamhshocraithe do gach ábhar slándála inmheánach agus seachtrach, lena n-áirítear iniúchtaí agus fiosruithe custaiméirí.

4.1.6 Ní mór dó/di faireachán a dhéanamh ar dhul chun cinn i gcoinne na gculpóirí sin le linn an athbhreithnithe bhliantúil. Ba cheart cuspóirí a bheith intomhaiste nuair is féidir (e.g. % den fhoireann a fuair oiliúint, líon na dteagmhas a tuairiscíodh, srl.) agus iad a athbhreithniú bunaithe ar fhionnachtana slándála agus ar athruithe riosca.

4.2 Fostaí Ainmnithe (más infheidhme)

4.2.1 Féadfaidh sé/sí tacú leis an mBainisteoir Ginearálta trí thascanna laethúla a bhainistiú, amhail cuntais úsáideoirí a chruthú, rochtain a bhaint de dhaoine a fhágann an eagraíocht, nó comhordú a dhéanamh leis an soláthraí TF.

4.2.2 Ní mór é/í a ainmniú go foirmiúil agus údarás agus uirlisí leordhóthanacha a bheith aige/aici chun na tascanna a chur i gcrích.

4.2.3 Tuairiscíonn sé/sí aon saincheisteanna don Bhainisteoir Ginearálta.

[... 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 Athbhreithniú bliantúil

9.1.1 Ní mór don Bhainisteoir Ginearálta (GM) athbhreithniú a dhéanamh ar an mbeartas seo uair sa bhliain ar a laghad chun comhlíonadh leanúnach cheanglais deimhniúcháin ISO/IEC 27001, athruithe rialála (amhail GDPR, NIS2 agus DORA), agus riachtanais ghnó atá ag teacht chun cinn a chinntiú.

9.2 Athbhreithnithe eatramhacha

9.2.1 Ní mór athbhreithnithe breise a dhéanamh aon uair a tharlaíonn athruithe suntasacha, amhail:

9.2.1.1 Mórtheagmhais slándála nó sáruithe

9.2.1.2 Próisis ghnó nó teicneolaíochtaí nua a thabhairt isteach (e.g. bogearraí nua, ardáin cianoibre, nó seirbhísí néalríomhaireachta)

9.2.1.3 Athruithe ar cheanglais dhlíthiúla nó rialála a dhéanann difear do láimhseáil faisnéise

9.3 Doiciméadú athruithe

9.3.1 Ní mór gach athbhreithniú beartais agus gach athrú a dhoiciméadú go foirmiúil, agus dáta, cineál na leasuithe agus faomhadh an GM a shonrú go soiléir.

9.3.2 Ní mór taifead stairiúil de leaganacha an bheartais a chothabháil go slán chun éabhlóid an bheartais agus comhlíonadh a léiriú le linn iniúchtaí.

9.4 Athruithe a chur in iúl

9.4.1 Ní mór aon athruithe ar an mbeartas seo a chur in iúl go pras do gach fostaí, conraitheoir agus tríú páirtí ábhartha.

9.4.2 Ní mór leaganacha nuashonraithe den bheartas a dhéanamh inrochtana go héasca don phearsanra uile lena mbaineann (e.g. a dháileadh go leictreonach nó a chur ar taispeáint go fisiciúil san ionad oibre).

10. Beartais ghaolmhara agus nascachtaí

10.1 Tá dlúthnasc ag an mbeartas seo le beartais eile i sraith beartas FGBM na heagraíochta, go háirithe:

10.1.1 P2S – Beartas um Rólanna agus Freagrachtaí Rialachais: Soiléiríonn sé sannadh dualgas agus freagrachtaí slándála.

10.1.2 P4S – Beartas Rialaithe Rochtana: Sainíonn sé láimhseáil shlán rochtana ar fhaisnéis na cuideachta.

10.1.3 P8S – Beartas Feasachta agus Oiliúna um Shlándáil Faisnéise: Soláthraíonn sé treoirlínte riachtanacha maidir le hoiliúint agus feasacht foirne.

10.1.4 P17S – Beartas um Chosaint Sonraí agus Príobháideacht: Cinntíonn sé comhlíonadh GDPR agus dlíthe eile um chosaint sonraí.

10.1.5 P30S – Beartas um Fhreagairt do Theagmhais: Déantar cur síos ann ar na gníomhartha mionsonraithe is gá mar fhreagairt ar theagmhais slándála.

10.2 Soláthraíonn na beartais ghaolmhara seo treoir oibríochtúil shoiléir agus ní mór iad a chur i bhfeidhm i gcomhar lena chéile chun comhlíonadh iomlán cheanglais deimhniúcháin ISO/IEC 27001 a bhaint amach.

11. Caighdeáin agus creatáil tagartha

11.1 ISO/IEC 27001

11.1.1 Clásal 5.1 – Ceannaireacht agus tiomantas: Ceanglaítear tiomantas na hardbhainistíochta agus cuntasacht as éifeachtacht na slándála faisnéise laistigh den eagraíocht.

11.1.2 Clásal 5.2 – Beartas Slándála Faisnéise: Sainordáítear beartais shoiléire dhoiciméadaithe atá ailínithe le straitéis na heagraíochta agus le ceanglais chomhlíonta.

11.1.3 Clásal 5.3 – Rólanna agus freagrachtaí eagraíochtúla: Sainítear sannadh soiléir freagrachtaí slándála faisnéise ar fud na heagraíochta, rud atá riachtanach do rialachas éifeachtach agus do chomhlíonadh iniúchta.

11.1.4 Clásal 6.1 – Gníomhartha chun aghaidh a thabhairt ar rioscaí agus deiseanna: Cinntítear go ndéantar rioscaí slándála faisnéise a shainaithint, a mheas agus a chóireáil go córasach.

11.1.5 Clásal 8.1 – Pleanáil agus rialú oibríochtúil: Ceanglaítear ar an eagraíocht na próisis is gá chun cuspóirí slándála faisnéise a bhaint amach agus rioscaí gaolmhara a bhainistiú go héifeachtach a phleanáil agus a chur i bhfeidhm.

11.2 ISO/IEC 27002:2022 Rialuithe 5.1–5

11.2.1 Rialú larscríbhíne A 5.1 – Beartais maidir le slándáil faisnéise: Sonraítear beartas slándála faisnéise doiciméadaithe a chruthú agus a chur in iúl.

11.2.2 Rialú larscríbhíne A 5.2 – Rólanna slándála faisnéise: Soiléirítear agus sannfar go foirmiúil rólanna agus freagrachtaí slándála faisnéise do pháirtithe ábhartha.

11.2.3 Rialú larscríbhíne A 5.3 – Scaradh dualgas: Forfheidhmítear scaradh soiléir dualgas chun coinbheachtaí leasa agus rioscaí calaoise a laghdú agus faisnéis íogair á bainistiú.

11.2.4 Rialú larscríbhíne A 5.4 – Freagrachtaí bainistíochta: Sainordaítear go léireoidh an bhainistíocht tiomantas do shlándáil faisnéise trí mhaoirseacht ghníomhach agus leithdháileadh acmhainní.

11.2.5 Treisítear an gá atá le beartais, rólanna, freagrachtaí agus struchtúir rialachais slándála faisnéise atá doiciméadaithe go soiléir, rud a chinntíonn bainistíocht chomhsheasmhach agus inrianaitheacht iniúchta ar fud na heagraíochta.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plean clár slándála faisnéise: Ceanglaítear straitéisí agus beartais rialachais slándála faisnéise dhoiciméadaithe, a sholáthraíonn creat le haghaidh cur chun feidhme agus bainistíocht chomhsheasmhach.

11.3.2 PL-1 – Beartas pleanála slándála: Sainordaítear beartas pleanála slándála ar fud na heagraíochta chun oibriú slán agus ailíniú straitéiseach gníomhaíochtaí slándála faisnéise a threorú.

11.3.3 CA-1 – Beartas measúnaithe agus údaraithe slándála: Éilítear rólanna measúnaithe agus údaraithe atá sainithe go soiléir chun éifeachtacht leanúnach agus comhlíonadh cheanglais slándála faisnéise a chinntiú.

11.3.4 AC-1 – Beartas rialaithe rochtana: Ceanglaítear ar eagraíochtaí cleachtais agus freagrachtaí bainistíochta rochtana a shainiú, a dhoiciméadú agus a chur chun feidhme go soiléir.

11.4 GDPR an Aontais Eorpaigh (2016/679)

11.4.1 Airteagal 5(2) – Prionsabal na cuntasachta: Ceanglaítear ar eagraíochtaí comhlíonadh phrionsabail chosanta sonraí a léiriú, lena n-áirítear rólanna agus beartais dhoiciméadaithe maidir le freagrachtaí cosanta sonraí.

11.4.2 Airteagal 32 – Slándáil próiseála: Sainordaítear bearta teicniúla agus eagraíochtúla iomchuí a chur i bhfeidhm, lena n-áirítear freagrachtaí soiléire slándála, chun sonraí pearsanta a chosaint ar sháruithe agus ar rochtain neamhúdaraithe.

11.5 Treoir NIS2 an Aontais Eorpaigh (2022/2555)

11.5.1 Airteagal 21(2)(a) – Bearta bainistíochta riosca: Ceanglaítear socruithe soiléire rialachais, lena n-áirítear rólanna agus freagrachtaí sainithe maidir le slándáil faisnéise, atá riachtanach chun cibearrioscaí a bhainistiú go héifeachtach.

11.6 DORA an Aontais Eorpaigh (2022/2554)

11.6.1 Airteagal 9 – Bainistíocht riosca TFC: Éilítear ar eagraíochtaí rólanna agus freagrachtaí a bhaineann le bainistíocht riosca TFC a shannadh go soiléir, rud a neartaíonn athléimneacht agus ullmhacht leanúnachais gnó.

11.6.2 Airteagal 10 – Leanúnachas gnó TFC: Ceanglaítear cuntasacht shoiléir agus rólanna struchtúrtha chun athléimneacht agus leanúnachas TFC a chothabháil, ag cinntiú gur féidir le heagraíochtaí freagairt go hiontaofa ar shuaitheadh.

11.7 COBIT 2019

11.7.1 EDM03 – Barrfheabhsú riosca a chinntiú: Leagtar béim ar chuntasacht agus ar rólanna atá sainithe go soiléir i mbainistiú rioscaí eagraíochtúla, rud a sholáthraíonn rialachas láidir agus maoirseacht éifeachtach ar rioscaí slándála faisnéise.

11.7.2 APO13 – Slándáil a bhainistiú: Ceanglaítear ar eagraíochtaí freagrachtaí bainistíochta slándála a bhunú agus a chur in iúl go soiléir, ag cinntiú ailíniú le cuspóirí gnó agus le ceanglais rialála.

11.7.3 DSS05 – Seirbhísí slándála a bhainistiú: Éilítear rólanna struchtúrtha agus freagrachtaí soiléire i mbainistiú seirbhísí slándála, rud a chumasaíonn cur chun feidhme comhsheasmhach agus fíorú comhlíonta.