					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P06					Teideal an doiciméid: **Beartas Bainistíochta Riosca**							
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**	**Athbhreithnitheag**	**Úinéir an phróisis**

Formheasanna			
Ainm	**Post**	**Dáta**	**Síniú**

Ailínithe le caighdeáin agus rialacháin

Caighdeán/Rialachán	Clásal/Airteagal	Nóta
ISO/IEC 27001:2022	Clásail 6.1, 8.32, 10	Príomhghnéithe de shainaithint agus bainistiú riosca, comhtháthú i mbainistíocht athruithe, agus feabhsú leanúnach
ISO/IEC 27005:2024	Modheolaíocht iomlán shaolré an riosca	Próiseas iomlán bainistíochta riosca i gcomhréir leis an gcaighdeán
ISO 31000:2018	Prionsabail agus creat bainistíochta riosca	Prionsabail bainistíochta riosca glactha sa chreat
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Treoir agus struchtúr do mheasúnuithe riosca agus do rialachas riosca ilshraitheach
GDPR an Aontais Eorpaigh	Airteagail 24, 25, 32	Próisis agus rialuithe riosca maidir le cosaint sonraí
NIS2 an Aontais Eorpaigh	Airteagal 21(2)(a–d)	Oibleagáidí maidir le measúnú riosca agus slándáil
DORA an Aontais Eorpaigh	Airteagail 5, 6	Bainistiú rioscaí TFC agus athléimneacht oibríochtúil
COBIT 2019	APO12, MEA	Struchtúr agus maoirseacht bainistíochta riosca

1. Cuspóir

1.1 Leis an mbeartas seo bunaítear creat aontaithe foirmiúil chun rioscaí slándála faisnéise a shainaithint, a anailísiú, a mheas, a chóireáil, faireachán a dhéanamh orthu agus athbhreithniú a dhéanamh orthu ar fud na heagraíochta.

1.2 Cinntíonn sé cur i bhfeidhm comhsheasmhach cur chuige rioscabhunaithe a chosnaíonn rúndacht, sláine agus infhaighteacht sócmhainní faisnéise, i gcomhréir le Clásal 6.1 de ISO/IEC 27001:2022 agus ISO 31000:2018.

1.3 Comhtháthaíonn an beartas seo Bainistíocht Riosca Slándála Faisnéise i bpróisis chinnteoireachta na heagraíochta chun cuspóirí straitéiseacha inmheánacha agus ceanglais rialála sheachtracha a chomhlíonadh.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir le gach aonad eagraíochtúil, próiseas gnó, córas, pearsanra agus rannpháirtíocht tríú páirtí a bhfuil baint acu le láimhseáil, forbairt, stóráil nó bainistiú sócmhainní faisnéise.

2.2 Síneann an raon feidhme chuig sócmhainní fisiciúla, digiteacha agus scamallbhunaithe, lena n-áirítear sonraí struchtúrtha agus neamhstruchtúrtha, feidhmchláir, bonneagar, líonraí agus seirbhísí.

2.3 Cumhdaíonn sé rioscaí slándála faisnéise ar an leibhéal straitéiseach, oibríochtúil, tionscadail agus teicniúil, agus tá sé éigeantach do gach fostaí, conraitheoir agus soláthraí seirbhíse a bhfuil baint acu le gníomhaíochtaí an ISMS.

2.4 Ní mór bainistíocht riosca a chur i bhfeidhm sna cásanna seo a leanas:

2.4.1 Tionscadal nua nó cur chun feidhme córais

2.4.1.1 Athruithe suntasacha (m.sh. ailtireacht, úinéireacht, próisis)

2.4.1.2 Soláthraithe nua a ionduchtú agus comhaontuithe tríú páirtí

2.4.1.3 Freagairt do theagmhais agus athbhreithniú iartheagmhais

2.4.1.4 Athbhreithnithe riosca eagraíochtúla tréimhsiúla nó iniúchtaí

3. Cuspóirí

3.1 Próiseas bainistíochta riosca in-athdhéanta ar fud na heagraíochta a bhunú agus a chur chun feidhme bunaithe ar mhodheolaíochtaí ISO/IEC 27005 agus ISO 31000.

3.2 A chinntiú go ndéantar rioscaí a shainaithint, a anailísiú, a mheas agus a chóireáil trí mhodhanna struchtúrtha inrianaithe, lena n-áirítear úinéireacht riosca a shannadh agus iad a nascadh le rialuithe.

3.3 Clár rioscaí láraithe faoi rialú leaganacha agus Plean Cóireála Riosca a chothabháil, ina léirítear stádas reatha riosca, clúdach rialaithe agus dul chun cinn maolaithe.

3.4 Cinntí riosca a ailíniú leis an inghlacthacht riosca dhoiciméadaithe agus leis na leibhéil lamháltais, agus cinnteoireacht rialachais eolasach a chumasú maidir le glacadh, maolú, aistriú nó seachaint riosca.

3.5 Faireachán leanúnach a dhéanamh ar threochtaí riosca agus éifeachtacht na gcóireálacha riosca a chinntiú, agus coigeartuithe réamhghníomhacha a chumasú bunaithe ar éabhlóid bagairtí nó ar athrú gnó.

4. Róil agus freagrachtaí

4.1 An Bhainistíocht Fheidhmiúcháin / Bord Stiúrthóirí

4.1.1 Faomhann siad an creat bainistíochta riosca agus sainmhíníonn siad an inghlacthacht riosca agus na tairseacha lamháltais.

4.1.2 Údaraíonn siad straitéisí cóireála riosca do rioscaí iarmharacha a sháraíonn an lamháltas.

4.1.3 Leithdháileann siad acmhainní agus maoirseacht chun an clár bainistíochta riosca a oibriú go héifeachtach.

4.2 Bainisteoir an ISMS / Oifigeach Riosca

4.2.1 Tá úinéireacht aige ar an mbeartas seo agus coimeádann sé ailíniú leis na caighdeáin ISO/IEC 27001 agus ISO/IEC 27005.

4.2.2 Tá sé freagrach as próiseas measúnaithe riosca na heagraíochta agus cothaíonn sé an Clár Rioscaí agus an Plean Cóireála Riosca.

4.2.3 Cinntíonn sé athbhreithnithe tréimhsiúla agus ardú príomhrioscaí chuig an gCeannaireacht Fheidhmiúcháin nó chuig Coiste Stiúrtha an ISMS.

[... 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 Déanfar athbhreithniú ar an mbeartas seo agus ar an gcreat gaolmhar go bliantúil, nó:

9.1.1 Tar éis mórtheagmhais riosca nó teagmhais slándála

9.1.2 Tar éis athrú suntasach eagraíochtúil nó teicniúil

9.1.3 Mar fhreagairt ar thorthaí iniúchta nó ar cheanglais rialála nua

9.2 Tá an Bainisteoir ISMS, an tOifigeach Riosca agus an Fhoireann Chomhlíonta freagrach i gcomhpháirt as:

9.2.1 An timthriall athbhreithnithe a thionscnamh

9.2.2 Ionchur a bhailiú ó aonaid ghnó

9.2.3 Nósanna imeachta agus tairseacha a leasú de réir mar is gá

9.3 Déanfar gach leasú:

9.3.1 Faoi rialú leaganacha agus logáilte

9.3.2 A fhaomhadh ag an mBainistíocht Fheidhmiúcháin

9.3.3 A chur in iúl do pháirtithe leasmhara

9.3.4 A choinneáil sa stór iniúchta ar feadh íostréimhse 5 bliana

10. Beartais ghaolmhara agus naisc eatarthu

10.1 Tá an beartas seo idirspleách leis na beartais slándála faisnéise seo a leanas:

10.1.1 P1 – Beartas Slándála Faisnéise: Leagtar amach ann an tsamhail rialachais slándála fhoriomlán faoina n-oibríonn an beartas riosca seo.

10.1.2 P2 – Beartas maidir le Róil agus Freagrachtaí Rialachais: Sainmhínítear ann na húinéirí cuntasacha agus na sraitheanna rialachais dá dtagraítear sa Mhaitrís Ardaithe Riosca.

10.1.3 P5 – Beartas um Bainistiú Athruithe: Spreagann sé athmheasúnú riosca i ndáil le hathruithe bonneagair agus eagraíochtúla.

10.1.4 P13 – Beartas Aicmithe agus Lipéadaithe Sonraí: Tacaíonn sé le measúnú tionchair le linn sainaithint riosca.

10.1.5 P33 – Beartas Faireacháin Iniúchta agus Comhlíonta: Bailíochtaíonn sé comhlíonadh beartais, lena n-áirítear iomláine an Chláir Rioscaí agus fianaise ar chóireálacha.

11. Caighdeáin agus creataí tagartha

11.1 Tá an beartas seo ailínithe go sainráite leis na caighdeáin agus na creataí seo a leanas chun a chinntiú go gcomhlíonann sé dea-chleachtais idirnáisiúnta agus ionchais rialála maidir le bainistíocht riosca slándála faisnéise:

11.2 ISO/IEC 27001:

11.2.1 Clásal 6.1: Leagtar amach ann na ceanglais chun rioscaí agus deiseanna a shainaithint, lena n-áirítear saolré iomlán na measúnuithe agus na gcóireálacha riosca slándála faisnéise. Cuireann an beartas seo Clásal 6.1.2 agus 6.1 i bhfeidhm trí chreat struchtúrtha a éilíonn prótacail dhoiciméadaithe maidir le sainaithint, anailís, meastóireacht, cóireáil agus glacadh le riosca iarmharach.

11.2.2 Clásal 8.32: Cinntíonn comhtháthú na smaointeoireachta rioscabhunaithe i bpróisis bhainistíochta athruithe go spreagann gach athrú suntasach eagraíochtúil athmheasúnuithe foirmiúla riosca.

11.2.3 Clásal 10: Tá feabhsú leanúnach leabaithe trí athbhreithnithe rialta ar bheartais, anailís ar threochtaí riosca agus nuashonruithe SoA atá bunaithe ar léargais riosca.

11.3 ISO/IEC 27005:

11.3.1 Soláthraíonn sé treoir shainiúil mhionsonraithe maidir le bainistíocht riosca slándála faisnéise. Cuireann an beartas seo samhail phróisis riosca iomlán ISO/IEC 27005 i bhfeidhm: Bunú Comhthéacs, Sainaithint Riosca, Anailís Riosca, Meastóireacht Riosca, Cóireáil Riosca, Glacadh le Riosca, Cumarsáid Riosca, Faireachán agus Athbhreithniú Riosca.

11.4 ISO 31000:

11.4.1 Comhtháthaíonn an beartas seo prionsabail ISO 31000 amhail tiomantas ceannaireachta, comhtháthú leis an gcinnteoireacht agus feabhsú leanúnach. Cinntíonn sé go bhfuil bainistíocht riosca leabaithe i gcultúr agus in oibríochtaí na heagraíochta.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Tá sé ailínithe le treoir NIST maidir le measúnuithe riosca a dhéanamh, lena n-áirítear sainaithint bagairtí, anailís leochaileachta, meastachán dóchúlachta agus cinneadh tionchair. Léiríonn struchtúr an bheartais seo na céimeanna measúnaithe riosca atá sainmhínithe ag NIST agus oiriúnaíonn sé iad do phróisis theicniúla agus ghnó araon.

11.6 NIST SP 800-39:

11.6.1 Tacaíonn sé le rialachas riosca ar leibhéal na heagraíochta, agus béim á leagan ar bhainistíocht riosca ilshraitheach ar leibhéal na heagraíochta, ar leibhéal próisis misean/próisis ghnó, agus ar leibhéal an chórais faisnéise. Cinntíonn an beartas seo go bhfuil úinéireacht riosca sainmhínithe go soiléir ag gach leibhéal agus go n-áirítear straitéisí cóireála ar leibhéal na heagraíochta.

11.7 GDPR an Aontais Eorpaigh:

11.7.1 Airteagal 24: Éilíonn sé bearta teicniúla agus eagraíochtúla cuí a chur i bhfeidhm chun a chinntiú go ndéantar rioscaí cosanta sonraí a bhainistiú i gceart — tugtar aghaidh air sin trí phróiseas riosca struchtúrtha an bheartais seo.

11.7.2 Airteagal 25: Tá “cosaint sonraí de réir dearaidh agus de réir réamhshocraithe” ailínithe le cóireáil riosca a leabú i ndearadh córas agus próiseas.

11.7.3 Airteagal 32: Sainordaítear cur chuige rioscabhunaithe i leith bearta slándála — comhlíontar é sin trí mheastóireachtaí riosca bunaithe ar thionchar agus roghnú rialuithe.

11.8 Treoir AE NIS2:

11.8.1 Airteagal 21(2)(a–d): Éilítear ar eintitis measúnuithe riosca a dhéanamh, beartais maidir le hanailís riosca a chur i bhfeidhm, agus bearta slándála comhréireacha a chinntiú. Comhlíonann an beartas seo na hoibleagáidí sin trí chur chun feidhme leanúnach shaolré an riosca agus trí rialachas doiciméadaithe.

11.9 DORA an Aontais Eorpaigh:

11.9.1 Airteagal 5: Sainordaítear creat doiciméadaithe bainistíochta rioscaí TFC — cumhdaítear go hiomlán é le hailtireacht an bheartais seo, lena n-áirítear mapáil SoA agus príomhtháscairí riosca.

11.9.2 Airteagal 6: Éilítear comhtháthú bainistíochta riosca i straitéisí athléimneachta oibríochtúla, agus tugtar aghaidh air sin trí mhaitrísí ardaithe agus rianú sócmhainní criticiúla.

11.10 COBIT 2019:

11.10.1 APO12 – Bainistiú Riosca: Mapálann sé go díreach le cur chuige struchtúrtha bainistíochta riosca na heagraíochta, trí róil a shannadh, cóireálacha a rianú agus cuntasacht a chinntiú ar leibhéal an Bhoird.

11.10.2 MEA01 – Faireachán, Meastóireacht agus Measúnú ar Fheidhmíocht agus ar Chomhréireacht: Léirítear é sin i bhfócas an bheartais seo ar anailís treochta, faireachán ar phríomhtháscairí riosca, agus comhtháthú aiseolais iniúchta i dtimthriallta feabhsúcháin leanúnaigh.