					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P06S					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**

Ailíniú le caighdeáin agus rialacháin

Caighdeán/Rialachán	Clásal/Airteagal	Nóta
ISO/IEC 27001:2022	Clásail 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev. 5	RA-1 go RA-7, PM-9	
Treoir NIS2 an AE	Airteagal 21(2)(a–d)	
DORA an AE	Airteagal 5	
COBIT 2019	APO12, MEA01	

1. Cuspóir

1.1 Sainmhínítear sa bheartas seo an chaoi a ndéanann an eagraíocht rioscaí a bhaineann le slándáil faisnéise, oibríochtaí, teicneolaíocht agus seirbhísí tríú páirtí a shainaithint, a mheasúnú agus a bhainistiú.

1.2 Cinntítear leis go bhfuil bainistíocht riosca ina cuid ghníomhach den phleanáil, de chur chun feidhme tionscadal, de roghnú soláthraithe agus d'fhragairt do theagmhais, i gcomhréir le ISO 27001, ISO 31000 agus ceanglais rialála.

1.3 Tacaíonn an beartas le cinnteoireacht eolasach, le cosaint sócmhainní faisnéise agus le hathléimneacht croí-oibríochtaí gnó.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir le:

2.1.1 gach roinn, córas agus úsáideoir laistigh den eagraíocht

2.1.2 gach faisnéis, seirbhís agus sócmhainn a bhainistítear go hinmheánach nó trí thríú páirtithe

2.1.3 gníomhaíochtaí a bhaineann le riosca, lena n-áirítear athbhreithnithe tionscadail, uasghráduithe córas, seachfhoinsiú agus comhlíonadh rialála

2.2 Áirítear leis gach cineál riosca, amhail:

2.2.1 bagairtí cibearshlándála agus leochaileachtaí córas

2.2.2 cur isteach oibríochtúil agus briseadh seirbhíse

2.2.3 nochtadh dlíthiúil, comhlíonta nó clú

2.2.4 rioscaí tríú páirtí agus rioscaí slabhra soláthair

2.3 Ní mór do gach fostaí, conraitheoir agus soláthraí seirbhíse an beartas seo a leanúint agus rioscaí á sainaithint nó á dtuairisciú acu.

3. Cuspóirí

3.1 Nósanna imeachta measúnaithe riosca atá simplí agus in-athdhéanta a chomhtháthú i ngnáthoibríochtaí gnó.

3.2 Rioscaí a d'fhéadfadh tionchar a imirt ar rúndacht, sláine, infhaighteacht nó ar chomhlíonadh dlíthiúil a shainaithint agus a chur in ord tosaíochta.

3.3 Úinéireacht a shannadh agus gníomhaíochtaí cóireála a shainmhíniú do gach riosca suntasach.

3.4 Clár rioscaí atá cruinn agus cothrom le dáta a chothabháil chun tacú le hullmhacht iniúchta agus le rianú rioscaí.

3.5 A chinntiú go bhfuil an bhainistíocht rannpháirteach i bhformheas lamháltas riosca agus i mórphleananna cóireála.

4. Róil agus freagrachtaí

4.1 An Bainisteoir Ginearálta

4.1.1 Socraíonn sé/sí goile riosca na heagraíochta agus formheasann sé/sí an creat bainistíochta riosca.

4.1.2 Formheasann sé/sí mórchinntí maidir le cóireáil riosca agus acmhainní.

4.1.3 Déanann sé/sí athbhreithniú ráithiúil ar na príomhrioscaí leis an gComhordaitheoir Riosca.

4.2 An Comhordaitheoir Riosca (nó Úinéir an ISMS)

4.2.1 Éascaíonn sé/sí measúnuithe riosca agus cothabhálann sé/sí an Clár Rioscaí.

4.2.2 Cinntíonn sé/sí go ndéantar scóráil riosca, úinéireacht agus gníomhaíochtaí cóireála a dhoiciméadú.

4.2.3 Eagraíonn sé/sí athbhreithniú foirmiúil riosca uair amháin sa bhliain ar a laghad.

[... 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 ar an mbeartas

9.1.1 Ní mór don Bhainisteoir Ginearálta agus don Chomhordaitheoir Riosca athbhreithniú a dhéanamh ar an mbeartas seo uair amháin sa bhliain ar a laghad chun a ábharthacht agus a iomláine a chinntiú.

9.2 Truicir nuashonraithe

9.2.1 Ní mór athbhreithniú agus nuashonrú luath a dhéanamh más rud é:

9.2.1.1 go nochtann mórtheagmhas nó toradh iniúchta bearnaí riosca

9.2.1.2 go dtugtar isteach aonaid ghnó nua, teicneolaíochtaí nua nó comhpháirtíochtaí nua

9.2.1.3 go n-athraíonn ceanglas rialála nó conarthach

9.3 Rialú leaganacha

9.3.1 Ní mór gach nuashonrú ar an mbeartas seo a leaganú leis na meiteashonraí seo a leanas:

9.3.1.1 uimhir an leagain agus an dáta éifeachta

9.3.1.2 achoimre ar na hathruithe

9.3.1.3 formheastóir (an Bainisteoir Ginearálta)

9.3.1.4 leaganacha roimhe seo curtha i gcartlann chun críocha iniúchta

9.4 Cumarsáid agus feasacht

9.4.1 Ní mór leaganacha nuashonraithe den bheartas agus mórphleananna cóireála riosca a chur in iúl don fhoireann ábhartha. Ní mór bunphrionsabail feasachta riosca a áireamh san oiliúint bhliantúil feasachta.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 Oibríonn an beartas seo i gcomhar le roinnt beartas eile chun rialachas slándála cuimsitheach a chinntiú:

10.1.1 P2S – Beartas Rólanna agus Freagrachtaí Rialachais: Sainmhíníonn sé cé atá cuntasach as úinéireacht riosca agus as cinnteoireacht.

10.1.2 P5S – Beartas um Bainistiú Athruithe: Éilíonn sé measúnú riosca sula gcuirtear athruithe teicniúla nó próisis chun feidhme.

10.1.3 P17S – Beartas um Chosaint Sonraí agus Príobháideachas: Pléann sé riosca rialála a bhaineann le láimhseáil sonraí pearsanta.

10.1.4 P30S – Beartas um Fhreagairt do Theagmhais: Cinntíonn sé go leanann cóireáil riosca le linn agus i ndiaidh teagmhais slándála.

10.1.5 P33S – Beartas Leanúnachais Gnó: Sainaithníonn sé rioscaí iarmharacha agus bearta téarnaimh le haghaidh seirbhísí criticiúla.

11. Caighdeáin tagartha agus creatlacha

11.1 ISO/IEC 27001:

11.1.1 Clásal 6.1 – Bunaíonn sé próiseas foirmiúil bainistíochta riosca agus pleanáil cóireála.

11.1.2 Clásal 6.1.3 – Éilíonn sé ar eagraíochtaí pleananna cóireála agus formheasanna doiciméadaithe a chothabháil.

11.2 ISO/IEC 27002:

11.2.1 Rialuithe 5.4, 5.25 – Soláthraíonn siad treoir cur chun feidhme maidir le húinéireacht riosca, tosaíochtú agus bainistíocht saolré.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 RA-1 go RA-7 – Sainmhíníonn siad measúnú riosca, straitéisí freagartha, doiciméadú agus sásraí athbhreithnithe.

11.4 PM-9 – Éilíonn sé maoirseacht chomhsheasmhach ar rioscaí eagraíochtúla ar leibhéal bainistíochta.

11.5 Treoir NIS2 an AE

11.5.1 Airteagal 21(2)(a–d) – Forchuireann sé rialuithe éigeantacha maidir le measúnú riosca, maolú agus rialachas ar eintitis riachtanacha agus thábhachtacha.

11.6 DORA an AE

11.6.1 Airteagal 5 – Éilíonn sé ar eintitis rialáilte creatlacha bainistíochta riosca TFC a shainmhíniú agus a bhainistiú, lena n-áirítear sainaithint, aicmiú agus freagairt.

11.7 COBIT 2019

11.7.1 APO12 – Bainistiú Riosca: Comhtháthaíonn sé riosca leis an bpleanáil straitéiseach agus oibríochtúil.

11.7.2 MEA01 – Faireachán, Meastóireacht agus Measúnú: Cinntíonn sé éifeachtacht agus comhlíonadh próiseas agus gníomhaíochtaí riosca.