					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P33					Teideal an doiciméid: **Beartas Faireacháin Iniúchta agus Comhlíonta**						
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 9.2, 9.3, 10	
ISO/IEC 27002:2022	Rialuithe 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
GDPR an Aontais Eorpaigh	Airteagail 24, 32, 33	
NIS2 an Aontais Eorpaigh	Airteagal 21(2)(g), 27	
DORA an Aontais Eorpaigh	Airteagail 10(2)(e), 25	
COBIT 2019	MEA01, MEA03	

1. Cuspóir

1.1 Is é cuspóir an bheartais seo clár faireacháin iniúchta agus comhlíonta na heagraíochta a bhunú agus a rialú chun:

1.1.1 Éifeachtacht rialuithe slándála agus príobháideachais a bhailíochtú

1.1.2 A chinntiú go bhfuil ailíniú ann leis na caighdeáin is infheidhme, leis na creataí dlíthiúla agus leis na hoibleagáidí conarthacha

1.1.3 Neamhchomhréireachtaí, neamhéifeachtúlachtaí agus rioscaí comhlíonta a bhrath go tráthúil

1.1.4 Tacú le feabhsú leanúnach agus le hullmhacht do dheimhnithe, do mheasúnuithe agus d'athbhreithnithe rialála

1.2 Tacaíonn an beartas seo le sláine agus aibíocht an Chórais Bainistíochta Slándála Faisnéise (ISMS) trí chleachtais struchtúrtha iniúchta agus faireacháin atá bunaithe ar riosca agus ar fhianaise a leabú ann.

2. Raon feidhme

2.1 Baineann an beartas seo le gach ceann díobh seo a leanas:

2.1.1 Aonaid ghnó inmheánacha, feidhmeanna agus ranna

2.1.2 Saoráidí fisiciúla, timpeallachtaí néalríomhaireachta, ardáin SaaS agus seirbhísí seachfhoinsithe

2.1.3 Córais faisnéise, feidhmchláir, bonneagar agus sócmhainní sonraí atá faoi raon feidhme an ISMS

2.1.4 Fostaithe, conraitheoirí agus soláthraithe seirbhíse tríú páirtí a bhfuil oibleagáidí iniúchta nó comhlíonta orthu

2.2 Cumhdaíonn an beartas:

2.2.1 Iniúchtaí inmheánacha

2.2.2 Iniúchtaí seachtracha/deimhniúcháin

2.2.3 Faireachán teicniúil ar chomhlíonadh

2.2.4 Iniúchtaí ar sholáthraithe agus ar thríú páirtithe

2.2.5 Gníomhartha ceartaitheacha agus coisctheacha (CAPA)

2.2.6 Méadrachtaí, painéil agus próisis tuairiscithe

2.3 Tá feidhm aige maidir leis na creataí ábhartha uile a bhfuil an eagraíocht faoina réir, lena n-áirítear ISO/IEC 27001, GDPR, NIS2, DORA agus SOC 2, i measc eile.

3. Cuspóirí

3.1 Leordhóthanacht agus éifeachtacht na rialuithe, na mbeartas agus na nósanna imeachta atá curtha chun feidhme ar fud an ISMS agus timpeallachtaí gaolmhara a fhíorú.

3.2 Aon easnaimh, neamhchomhréireachtaí nó bearnaí comhlíonta a shainaithint agus a leigheas sula n-ardóidh siad go teagmhais nó sáruithe.

3.3 Ullmhacht leanúnach a chinntiú d'athbhreithnithe inmheánacha rialachais, d'iniúchtaí seachtracha agus do dheimhnithe neamhspleácha.

3.4 Fianaise chosanta agus rianta iniúchta a chruthú chun tacú le fiosrúcháin rialála, próisis dlí nó iarratais ó chustaiméirí ar dhearbhú.

3.5 Torthaí iniúchta a chomhtháthú le bainistíocht riosca níos leithne na heagraíochta, le méadrachtaí slándála agus le gníomhaíochtaí feabhsaithe leanúnaí.

4. Róil agus freagrachtaí

4.1 Ceannaire an Iniúchta Inmheánaigh / Bainisteoir Comhlíonta

4.1.1 Déanann sé/sí iniúchtaí inmheánacha a phleanáil, a sceidealú agus a chur i gcrích bunaithe ar thosaíocht riosca.

4.1.2 Coinníonn sé/sí an Clár Iniúchta, comhordaíonn sé/sí gníomhaíochtaí iniúchta agus déanann sé/sí obair leantach ar ghníomhartha ceartaitheacha.

4.2 Príomhoifigeach Slándála Faisnéise (CISO)

4.2.1 Cinntíonn sé/sí go gcumhdaíonn raon feidhme an iniúchta gach eilimint ábhartha den ISMS agus rialuithe Iarscríbhinn A.

4.2.2 Déanann sé/sí maoirseacht ar bhailíochtú CAPA agus comhtháthaíonn sé/sí torthaí iniúchta sa chlár slándála.

[... 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 Ní mór don Bhainisteoir Comhlíonta agus don CISO athbhreithniú a dhéanamh ar an mbeartas seo ar a laghad uair sa bhliain, nó níos luaithe mar fhreagairt ar:

9.1.1 Athruithe i gcreataí rialála, conarthacha nó deimhniúcháin

9.1.2 Torthaí suntasacha iniúchta nó teipeanna rialaithe athfhillteacha

9.1.3 Athstruchtúrú eagraíochtúil nó athruithe ar an gcóras GRC

9.1.4 Moltaí ó iniúchóirí seachtracha nó aiseolas ó rialálaithe

9.2 Ní mór don phróiseas athbhreithnithe measúnú a dhéanamh ar:

9.2.1 Modheolaíocht phleanála iniúchta agus minicíocht

9.2.2 Athruithe ar raon feidhme an ISMS nó ar an mbonneagar

9.2.3 Nuashonruithe ar chatalóg na rialuithe nó ar an gclár dlíthiúil

9.2.4 Comhsheasmhacht agus cáilíocht fhianaise iniúchta agus phróisis CAPA

9.3 Ní mór gach athrú beartais a bheith:

9.3.1 Doiciméadaithe i stór faoi rialú leaganacha

9.3.2 Formheasta ag an mBainistíocht Feidhmiúcháin

9.3.3 Curtha in iúl don phearsanra uile lena mbaineann agus comhtháite i nósanna imeachta nuashonraithe agus i gcláir feasachta

9.4 Ní mór don bhailíochtú iar-athbhreithnithe a dheimhniú go léirítear ceanglais nuashonraithe sa Chlár Iniúchta, in uirlisí comhlíonta agus i bpainéil inmheánacha faireacháin.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 Tá an beartas seo ailínithe leis na beartais eagraíochtúla ghaolmhara seo a leanas:

10.1.1 P1 – Beartas Slándála Faisnéise: Sainmhíníonn sé an ISMS agus bunaíonn sé cuntasacht as comhlíonadh agus feabhsú leanúnach

10.1.2 P5 – Beartas um Bainistiú Athruithe: Cinntíonn sé infheictheacht iniúchta ar athruithe bonneagair agus cumraíochta a théann i bhfeidhm ar thimpeallachtaí rialaithe

10.1.3 P6 – Beartas Bainistíochta Riosca: Comhtháthaíonn sé torthaí iniúchta i ngníomhaíochtaí meastóireachta agus cóireála riosca ar fud na heagraíochta

10.1.4 P14 – Beartas um Choinneáil agus Diúscairt Sonraí: Rialaíonn sé coinneáil fianaise iniúchta, logaí agus taifid chomhlíonta

10.1.5 P18 – Beartas Rialuithe Cripteagrafacha: Tacaíonn sé le stóráil agus aistriú slán sonraí iniúchta íogaire

10.1.6 P26 – Beartas Slándála Tríú Páirtí agus Soláthraithe: Cumhdaíonn sé cearta iniúchta, doiciméadacht dearbhaithe agus maoirseacht ar chomhlíonadh díoltóirí

10.1.7 P30 – Beartas Freagartha do Theagmhais: Ailíníonn sé iniúchtaí ar phróisis láimhseála teagmhas le cuspóirí dearbhaithe an ISMS

10.1.8 P32 – Beartas Leanúnachais Gnó agus Athshlánaithe ó Thubaiste: Éilíonn sé fíorú ar thástáil leanúnachais agus ar chomhlíonadh DRP le linn timthriallta iniúchta

11. Caighdeáin agus creataí tagartha

11.1 Tá an beartas seo ailínithe le caighdeáin idirnáisiúnta agus ceanglais dhlíthiúla maidir le hiniúchadh agus bailíochtú leanúnach ar chomhlíonadh.

11.2 ISO/IEC 27001:

11.2.1 Clásal 9.2 – Iniúchadh inmheánach: Éilíonn sé iniúchtaí rialta, bunaithe ar riosca, ar an ISMS chun éifeachtacht agus comhréireacht a mheas.

11.2.2 Clásal 9.3 – Athbhreithniú bainistíochta: Ní mór torthaí iniúchta a chur san áireamh san athbhreithniú straitéiseach agus san fheabhsú.

11.2.3 Clásal 10.1 – Neamhchomhréireacht agus gníomhartha ceartaitheacha: Ní mór aghaidh a thabhairt ar thorthaí iniúchta trí nósanna imeachta CAPA doiciméadaithe.

11.3 ISO/IEC 27002:2022 – Rialuithe 5.35–5.37:

11.3.1 Rialuithe Iarscríbhinn A 5.35–5.37: Cumhdaíonn siad athbhreithniú neamhspleách, comhlíonadh ceanglas dlíthiúil/conarthach, agus logáil iniúchta.

11.3.2 Soláthraíonn siad treoir chur chun feidhme maidir le cláir iniúchta agus comhlíonta a phleanáil, a chur i gcrích agus a fheabhsú.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – Measúnuithe rialaithe: Éilíonn sé athbhreithniú rialta ar rialuithe slándála atá curtha chun feidhme.

11.4.2 CA-5 – Plan of Action and Milestones (POA&M): Ailíníonn sé le rianú agus leigheas torthaí iniúchta.

11.4.3 CA-7 – Faireachán leanúnach: Tacaíonn sé le measúnuithe réamhghníomhacha uathoibrithe ar chomhlíonadh.

11.5 GDPR an Aontais Eorpaigh (2016/679):

11.5.1 Airteagail 24 agus 32: Sainordaíonn siad fianaise ar chur chun feidhme agus ar éifeachtacht rialuithe slándála trí struchtúir rialachais iomchuí.

11.5.2 Airteagal 33: Tacaíonn sé leis an ngá atá le rianta iniúchta bailí i bhfreagairt ar sháruithe agus i bhfógairt sáruithe.

11.6 Treoir NIS2 an Aontais Eorpaigh (2022/2555):

11.6.1 Airteagal 21(2)(g): Éilíonn sé iniúchadh ar bheartais agus ar nósanna imeachta mar chuid d'íosbhearta bainistíochta riosca cibearshlándála.

11.6.2 Airteagal 27: Féadfaidh údaráis náisiúnta iniúchtaí a dhéanamh nó a cheangal ar eintitis riachtanacha agus thábhachtacha.

11.7 DORA an Aontais Eorpaigh (2022/2554):

11.7.1 Airteagal 10(2)(e): Ní mór d'eintitis iniúchtaí inmheánacha agus seachtracha a dhéanamh ar chleachtais bainistíochta riosca TFC.

11.7.2 Airteagal 25 – Ceanglais iniúchta: Sainordaíonn sé iniúchtaí tréimhsiúla ag iniúchóirí inmheánacha nó neamhspleácha seachtracha le hinfheictheacht rialála.

11.8 COBIT 2019:

11.8.1 MEA01 – Monitor, Evaluate and Assess Performance and Conformance: Cinntíonn sé go ndéantar éifeachtacht rialuithe a fhíorú agus a thuairisciú do chomhlachtaí rialachais.

11.8.2 MEA03 – Monitor, Evaluate and Assess Compliance: Éilíonn sé ailíniú chleachtais eagraíochtúla le ceanglais dhlíthiúla, chonarthacha agus ceanglais atá bunaithe ar chaighdeáin.