					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P33S					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, 10	Iniúchtaí inmheánacha, feabhsú leanúnach agus ceartú neamhchomhréireachta
ISO/IEC 27002:2022	Rialuithe 5.35, 5.37	Athbhreithnithe inmheánacha sceidealta, athbhreithnithe neamhspleácha ar phróisis sheachfhoinsithe
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Measúnuithe slándála, faireachán leanúnach ar chomhlíonadh, athbhreithniú/anailís/tuairisciú iniúchta
GDPR an AE	Airteagail 24 agus 32	Iniúchadh ar rialuithe teicniúla agus eagraíochtúla (TOManna), fianaise ar éifeachtacht rialuithe
NIS2 an AE	Airteagal 21(2)(f)	Athbhreithniú réamhghníomhach agus comhlíonadh bunaithe ar fhianaise
DORA an AE	Airteagal 10	Bainistíocht riosca TFC, faireachán agus tuairisciú
COBIT 2019	MEA01, MEA03	Faireachán/measúnú comhréireachta, comhlíonadh, ullmhacht d'athbhreithnithe tríú páirtí

1. Cuspóir

1.1 Leis an mbeartas seo, bunaítear cur chuige na heagraíochta maidir le hiniúchtaí inmheánacha, seiceálacha ar rialuithe slándála agus faireachán ar chomhlíonadh rialála. Cinntítear leis go mbíonn gach rialú, beartas, córas agus soláthraí seirbhíse faoi réir athbhreithnithe rialta struchtúrtha.

1.2 Is é cuspóir an bheartais seo teipeanna rialaithe a bhrath, neamhchomhlíonadh a chosc agus dícheall cuí a léiriú faoi ISO/IEC 27001, GDPR agus creataí gaolmhara.

1.3 Cuireann sé seo ar chumas FGBManna rialú oibríochtúil agus ullmhacht deimhniúcháin a choinneáil, fiú mura bhfuil feidhm chomhlíonta thiomnaithe acu, trí sheicliostaí simplí in-athúsáidte agus fionnachtana a bhfuil tosaíocht riosca leo a úsáid.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir leis na nithe seo a leanas:

2.1.1 Gach roinn inmheánach agus gach soláthraí seirbhíse seachtrach a bhfuil freagrachtaí acu i ndáil le córais TF, sonraí pearsanta agus seirbhísí gnó criticiúla

2.1.2 Gach rialú agus córas atá laistigh de raon feidhme an Chórais Bainistíochta Slándála Faisnéise (ISMS)

2.1.3 Gach iniúchadh inmheánach, athbhreithniú ar rialuithe slándála agus seiceáil chomhlíonta, cibé acu a dhéantar go hinmheánach nó ag sainchomhairleoir seachtrach, cliant nó rialálaí

2.2 Tá feidhm ag an mbeartas seo freisin maidir le bailiú fianaise agus tuairisciú i gcás:

2.2.1 Iniúchtaí deimhniúcháin agus athdheimhniúcháin ISO/IEC 27001

2.2.2 Iniúchtaí cosanta sonraí faoi GDPR nó faoi théarmaí conarthacha

2.2.3 Ceistneoirí slándála arna dtionscnamh ag cliaint nó athbhreithnithe dícheall cuí

2.2.4 Aon athbhreithniú rialála nó neamhspleách faoi NIS2 nó DORA, más infheidhme

3. Cuspóirí

3.1 A chinntiú go ndéantar athbhreithniú rialta ar gach príomhrialú agus príomhbheartas maidir lena n-éifeachtacht agus a gcomhlíonadh.

3.2 Rian iniúchta agus taifid ar ghníomhartha ceartaitheacha a choinneáil chun cuntasacht agus feabhsú a léiriú.

3.3 Ullmhú do dheimhniúchán, athdheimhniúchán agus cláir dearbhaithe custaiméirí (m.sh. ISO 27001, ionduchtú soláthraithe).

3.4 Bearnaí a shainaithint go luath chun ceartú pras a chumasú sula n-ardóidh saincheisteanna nó sula sáraítear oibleagáidí.

3.5 A chur ar chumas an Bhainisteora Ghinearálta agus an tSoláthraí TF athbhreithnithe a chomhordú gan castacht neamhriachtanach, agus torthaí inchosanta á gcinntiú ag an am céanna.

4. Róil agus freagrachtaí

4.1 Bainisteoir Ginearálta (GM)

4.1.1 Déanann sé/sí maoirseacht ar an gclár iniúchta.

4.1.2 Formheasann sé/sí pleananna agus fionnachtana athbhreithnithe inmheánaigh.

4.1.3 Sannann agus rianaíonn sé/sí gníomhartha ceartaitheacha.

4.1.4 Údaraíonn sé/sí rannpháirtíocht iniúchóirí seachtracha nó sainchomhairleoirí.

4.2 Soláthraí TF / Riarthóir

4.2.1 Soláthraíonn sé/sí fianaise le linn iniúchtaí inmheánacha agus seachtracha (m.sh. logaí, cumraíochtaí, taifid rialaithe rochtana).

4.2.2 Tacaíonn sé/sí le seiceálacha teicniúla (m.sh. stádas cúltacaí, comhlíonadh paisteála).

4.2.3 Coinníonn sé/sí stór fianaise iniúchta.

[... 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 bheartas agus ar phlean iniúchta

9.1.1 Ní mór don Bhainisteoir Ginearálta (GM) athbhreithniú a dhéanamh ar an mbeartas seo agus ar an sceideal iniúchta ar a laghad uair sa bhliain.

9.1.2 Ní mór don athbhreithniú measúnú a dhéanamh ar:

9.1.2.1 Éifeachtacht na n-iniúchtaí maidir le bearnaí a shainaithint

9.1.2.2 Ráta críochnaithe na n-iniúchtaí agus na ngníomhartha ceartaitheacha

9.1.2.3 Athruithe ar na ceanglais dlíthiúla, rialála nó deimhniúcháin is infheidhme

9.2 Nuashonruithe bunaithe ar thruicear

9.2.1 Ní mór athbhreithniú agus nuashonrú a dhéanamh ar an mbeartas nuair:

9.2.2 A eascraíonn mór-neamhchomhréireacht as deimhniúchán nó cigireacht faireachais

9.2.3 A athraíonn creataí dlíthiúla nó rialála (m.sh. treoir nua GDPR, cur chun feidhme náisiúnta NIS2)

9.2.4 A dhéanann athruithe gnó difear do chórais, próisis nó díoltóirí atá laistigh de raon feidhme an iniúchta

9.2.5 A nochtann teagmhas criticiúil nó sárú bearnaí rialaithe nár braitheadh roimhe seo

9.3 Doiciméadú ar nuashonruithe

9.3.1 Ní mór gach leasú a rianú i loga rialaithe leaganacha an bheartais.

9.3.2 Ní mór nuashonruithe a dháileadh ar gach ball foirne a bhfuil baint acu le hiniúchtaí.

9.3.3 Ní mór achoimre ar na hathruithe a chur san áireamh leis an mbeartas nuashonraithe chun tuiscint a chinntiú.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 Tacaíonn roinnt beartas FGBM eile leis an mbeartas seo agus neartaíonn siad é:

10.1.1 P1S – Beartas Slándála Faisnéise: Leagann sé síos an bhonnlíne do gach ionchas rialaithe agus ceanglaíonn sé cur chun feidhme trí iniúchtaí.

10.1.2 P2S – Beartas um Róil agus Freagrachtaí Rialachais: Bunaíonn sé cuntasacht i leith pleanáil, cur i gcrích agus úinéireacht ghníomhartha ceartaitheacha iniúchta.

10.1.3 P6S – Beartas Bainistíochta Riosca: Aithníonn sé laigí rialaithe a thagann chun solais le linn iniúchtaí agus cinntíonn sé go ndéantar na fionnachtana a dhoiciméadú sa chlár rioscaí.

10.1.4 P17S – Beartas um Chosaint Sonraí agus Príobháideachas: Sainmhíníonn sé na rialuithe GDPR nach mór a iniúchadh, lena n-áirítear láimhseáil sonraí, freagairt ar sháruithe agus fógraí príobháideachais.

10.1.5 P22S – Beartas Logála agus Monatóireachta: Soláthraíonn sé na logaí iniúchta agus na sonraí fóiréinseacha a úsáidtear le linn athbhreithnithe comhlíonta agus rialaithe.

10.1.6 P30S – Beartas Freagartha do Theagmhais: Ceanglaíonn sé iniúchadh tréimhsiúil ar thaifid teagmhas agus ar athbhreithnithe iar-theagmhais chun éifeachtacht na freagartha a fhíorú.

10.1.7 P31S – Beartas maidir le Bailiú Fianaise agus Fóiréinsic: Soláthraíonn sé na nósanna imeachta chun fianaise infhíoraithe le slabhra coimeádta a bhailiú le linn iniúchtaí.

10.2 Le chéile, cruthaíonn na beartais seo timpeallacht rialaithe lúb dúnta a chumasaíonn fíorú inmheánach, dearbhú seachtrach agus rialachas atá ailínithe le caighdeáin.

11. Caighdeáin agus creataí tagartha

11.1 ISO/IEC 27001:

11.1.1 Clásal 9.2 – Ceanglaíonn sé iniúchtaí inmheánacha chun feidhmíocht an ISMS agus a ailíniú leis na ceanglais a mheas.

11.1.2 Clásal 10.1 – Ceanglaíonn sé feabhsú leanúnach bunaithe ar thorthaí iniúchta agus ar cheartú neamhchomhréireachta.

11.2 ISO/IEC 27002:

11.2.1 Rialú 5.35 – Ceanglaíonn sé athbhreithnithe inmheánacha sceidealta ar rialuithe agus ar phróisis.

11.2.2 Rialú 5.37 – Leagann sé béim ar athbhreithnithe neamhspleácha, go háirithe maidir le próisis sheachfhoinsithe.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Measúnuithe slándála: Ceanglaíonn sé iniúchtaí ar rialuithe curtha chun feidhme chun a n-éifeachtacht a fhíorú.

11.3.2 CA-7 – Faireachán leanúnach ar chomhlíonadh: Leagann sé béim ar bhrath agus ar athbhreithniú réamhghníomhach laigí rialaithe.

11.3.3 AU-6 – Athbhreithniú, Anailís agus Tuairisciú Iniúchta: Ceanglaíonn sé anailís rialta agus réiteach ar logaí iniúchta agus ar fhionnachtana.

11.4 GDPR an AE:

11.4.1 Airteagail 24 agus 32 – Ceanglaíonn siad cur chun feidhme agus iniúchadh ar rialuithe teicniúla agus eagraíochtúla, lena n-áirítear fianaise ar éifeachtacht rialuithe agus ar fheabhsú le himeacht ama.

11.5 Treoir NIS2 an AE (2022/2555):

11.5.1 Airteagail 20–21 – Ceanglaíonn siad athbhreithniú réamhghníomhach ar rialuithe, comhlíonadh bunaithe ar fhianaise agus iniúchthacht i gcás eintiteas riachtanach agus tábhachtach.

11.6 COBIT 2019:

11.6.1 MEA01 – Faireachán, Meastóireacht agus Measúnú ar Fheidhmíocht agus ar Chomhréireacht: Ceanglaíonn sé measúnú tréimhsiúil ar fheidhmíocht próiseas agus rialuithe i gcoinne caighdeán agus cuspóirí.

11.6.2 MEA03 – Comhlíonadh le Ceanglais Sheachtracha a Chinntiú: Díríonn sé ar fhaireachán inmheánach agus ar ullmhacht d'iniúchtaí tríú páirtí agus d'athbhreithnithe rialála.