					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P26					Teideal an doiciméid: **Beartas Slándála Tríú Páirtí agus Soláthraí - FBM**						
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	Clásal 8	Pleanáil agus Rialú Oibríochtúil: ceanglaítear rialuithe foirmiúla ar sheirbhísí tríú páirtí a mbíonn tionchar acu ar an ISMS
ISO/IEC 27002:2022	Rialuithe 5.19–5.22	Beartais agus nósanna imeachta maidir le caidrimh le soláthraithe; bainistiú riosca soláthraithe; bainistíocht seachadta seirbhíse soláthraithe; faireachán agus athbhreithniú ar sholáthraithe
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Seirbhísí córais sheachtracha; bainistíocht cumraíochta forbróra; idirnaisc chórais; slándáil pearsanra tríú páirtí
GDPR an Aontais Eorpaigh	Airteagail 28, 32, 33	Oibleagáidí próiseálaí; slándáil na próiseála; fógra faoi shárú sonraí pearsanta
NIS2 an Aontais Eorpaigh	Airteagal 21(2)(e–f)	Bainistíocht soláthraithe bunaithe ar riosca agus maoirseacht slándála
DORA an Aontais Eorpaigh	Airteagail 28, 30	Riosca TFC tríú páirtí; maoirseacht ar sholáthraithe criticiúla TFC tríú páirtí
COBIT 2019	BAI05, DSS02, MEA03	Cumasú athraithe eagraíochtúil a bhainistiú; iarratais seirbhíse agus teagmhais a bhainistiú; faireachán, meastóireacht agus measúnú ar chomhlíonadh

1. Cuspóir

1.1 Sainmhínítear sa bheartas seo na ceanglais slándála faisnéise chun caidrimh shlána a bhunú, a bhainistiú agus a chothabháil le soláthraithe tríú páirtí agus le soláthraithe seirbhíse.

1.2 Cinntítear leis go mbíonn gach soláthraí a bhfuil rochtain aige ar shonraí, ar chórais nó ar bhonneagar na heagraíochta faoi réir rialuithe slándála dochta, coimircí conarthacha agus maoirseacht leanúnach ar feadh shaolré na seirbhíse.

1.3 Tacaíonn an beartas seo le rialuithe Iarscríbhinn A de ISO/IEC 27001, 5.19 go 5.22, trí cheanglais slándála a leabú i soláthar, i ndícheall cuí soláthraithe, in ionduchtú, i mbainistíocht conarthaí, i bhfaireachán seirbhíse agus i bpróisis fhoirceanta.

2. Raon feidhme

2.1 Baineann an beartas seo leis na nithe seo a leanas:

2.1.1 Gach soláthraí tríú páirtí, conraitheoir, soláthraí scamall agus eagraíocht seirbhíse a phróiseálann nó a fhaigheann rochtain ar shócmhainní faisnéise na heagraíochta

2.1.2 Gach ról inmheánach atá bainteach le measúnú soláthraithe, ionduchtú, conarthú, bainistíocht riosca, faireachán nó foirceannadh

2.1.3 Gach caidreamh le soláthraithe a chuimsíonn rochtain ar shonraí íogaire, comhtháthú le seirbhísí táirgthe, nó tacaíocht d'fheidhmeanna gnó criticiúla

2.2 Clúdaítear leis seo soláthraithe díreacha agus a bhfophhróiseálaithe nuair is infheidhme, agus áirítear ann bogearraí tríú páirtí, bonneagar, tacaíocht agus seirbhísí seachfhoinsithe.

3. Cuspóirí

3.1 A chinntiú go sainaithnítear, go measúnaítear agus go maolaítear rioscaí slándála soláthraithe go comhsheasmhach ar feadh shaolré an chaidrimh.

3.2 Ceanglais chaighdeánaithe slándála a leabú i ngach conradh soláthraithe, lena n-áirítear oibleagáidí fógra faoi shárú, téarmaí maidir leis an gceart iniúchta agus freagrachtaí cosanta sonraí.

3.3 A cheangal go ndéanfar dícheall cuí foirmiúil agus measúnuithe riosca doiciméadaithe sula ngabhfar do sholáthraithe nua nó sula ndéanfar comhaontuithe seirbhíse ardriosca a athnuachan.

3.4 Sásraí a bhunú le haghaidh faireachán leanúnach ar chomhlíonadh soláthraithe, lena n-áirítear athbhreithnithe feidhmíochta, iniúchtaí agus uaschéimniú teagmhas.

3.5 Athruithe ar sheirbhísí soláthraithe a bhainistiú agus eisduchtú slán mar aon le sonraí a thabhairt ar ais nó a scriosadh a chur chun feidhme tráth foirceanta.

3.6 Rialuithe slándála tríú páirtithe a ailíniú leis na hoibleagáidí rialála agus conarthacha is infheidhme, lena n-áirítear GDPR, NIS2, DORA agus caighdeáin ISO/IEC 27001.

4. Róil agus freagrachtaí

4.1 Príomhoifigeach Slándála Faisnéise (CISO)

4.1.1 Is leis an oifigeach seo an beartas seo agus cinntíonn sé go bhfuil sé ailínithe leis an ISMS foriomlán, leis an straitéis bainistíochta riosca agus leis an straitéis chomhlíonta.

4.1.2 Formheasann sé aicmiú agus sraitheanna riosca soláthraithe, torthaí athbhreithnithe slándála agus eisceachtaí ardriosca.

4.1.3 Glacann sé páirt in uaschéimniú teagmhas tromchúiseach a bhaineann le soláthraithe agus i gcaibidlíocht conarthaí le haghaidh seirbhísí criticiúla.

4.2 Soláthar agus bainistíocht soláthraithe

4.2.1 Cinntíonn siad go gcuirtear clásail cheadaithe slándála agus cosanta sonraí san áireamh i ngach conradh soláthraithe nua agus athnuaite.

4.2.2 Coinníonn siad an clár láraithe soláthraithe agus comhordaíonn siad leis an bhfeidhm Dlí agus Comhlíonta maidir le doiciméadacht riosca tríú páirtí.

4.2.3 Tionscnaíonn siad próisis ionduchtaithe agus cinntíonn siad ailíniú le measúnuithe slándála réamhchonartha.

[... 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 athbhreithniú a dhéanamh ar an mbeartas seo uair sa bhliain ar a laghad, nó níos luaithe i gcás:

9.1.1 Athruithe ábhartha ar straitéis an tsoláthair nó ar éiceachóras na soláthraithe

9.1.2 Nuashonruithe ar chreataí dlíthiúla nó rialála (m.sh. DORA, GDPR)

9.1.3 Teagmhais mhóra tríú páirtí, sáruithe sonraí nó teipeanna iniúchta

9.1.4 Torthaí ó mheasúnuithe riosca nó ó chomhlachtaí deimhniúcháin seachtracha

9.2 Is comhúinéirí ar an bpróiseas athbhreithnithe iad an CISO, Soláthar, Dlí agus na feidhmeanna Bainistíochta Riosca.

9.3 Ní mór gach leasú ar an mbeartas a dhoiciméadú i gClár Rialaithe Doiciméad an ISMS, a chur faoi rialú leaganacha, agus a chur in iúl do pháirtithe leasmhara ábhartha trí bhealaí rialachais soláthraithe agus trí chláir feasachta fostaithe.

9.4 Ní mór leaganacha a cuireadh in ionad a chartlannú ar feadh trí bliana ar a laghad ar mhaithe le hinrianaitheacht agus comhlíonadh dlíthiúil.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 P1 – Beartas Slándála Faisnéise. Leagtar síos ann an gealltanas foriomlán gach oibríocht eagraíochtúil a dhaingniú, lena n-áirítear spleáchas ar sholáthraithe tríú páirtí agus ar sholáthraithe seachtracha seirbhísí TF.

10.2 P6 – Beartas Bainistíochta Riosca. Treoraíonn sé sainaithint, measúnú agus maolú rioscaí a bhaineann le caidrimh tríú páirtithe, lena n-áirítear rioscaí oidhreachta nó sistéamacha ó éiceachórais soláthraithe.

10.3 P17 – Beartas um Chosaint Sonraí agus Príobháideachas. Baineann sé le gach soláthraí a láimhseálann sonraí pearsanta, agus éilíonn sé téarmaí conarthacha iomchuí, coimircí aistrithe agus prionsabail phríobháideachais trí dhearadh.

10.4 P4 – Beartas Rialaithe Rochtana. Rialaíonn sé an chaoi a bhfaigheann pearsanra tríú páirtí rochtain ar chórais na heagraíochta, agus cuireann sé ceadanna rólbhunaithe, rialuithe seisiúin agus nósanna imeachta aisghairme i bhfeidhm.

10.5 P22 – Beartas Logála agus Monatóireachta. Éilíonn sé go ndéanfar faireachán, logáil agus athbhreithniú ar rochtain soláthraithe ar chórais, go háirithe i dtimpeallachtaí ina dtarlaíonn gníomhaíochtaí pribhléideacha nó gníomhaíochtaí atá dírithe ar shonraí.

10.6 P30 – Beartas Freagartha do Theagmhais. Sainmhínítear ann nósanna imeachta uaschéimnithe agus ceanglais tuairiscithe sáraithe maidir le teagmhais slándála ar tionscnaíodh iad ag soláthraithe nó maidir le himscrúduithe comhpháirteacha a bhaineann le córais tríú páirtí.

11. Caighdeáin agus creataí tagartha

11.1 ISO/IEC 27001: Clásal 8.1 – Pleanáil agus Rialú Oibríochtúil: ceanglaítear rialuithe foirmiúla ar sheirbhísí tríú páirtí a mbíonn tionchar acu ar an ISMS.

11.2 ISO/IEC 27002:2022 – Rialuithe 5.19 go 5.22:

11.2.1 Rialú Iarscríbhinn A 5.19 – Beartais agus nósanna imeachta maidir le caidrimh le soláthraithe: sainordaítear rialuithe chun idirghníomhaíochtaí le soláthraithe a bhainistiú.

11.2.2 Rialú Iarscríbhinn A 5.20 – Bainistiú riosca soláthraithe: dírítear ar shainaithint, measúnú agus maoirseacht leanúnach ar staid slándála soláthraithe.

11.2.3 Rialú Iarscríbhinn A 5.21 – Bainistíocht seachadta seirbhíse soláthraithe: ceanglaítear ailíniú feidhmíochta agus slándála le hionchais chonarthacha.

11.2.4 Rialú Iarscríbhinn A 5.22 – Faireachán agus athbhreithniú ar sholáthraithe: treisítear an gá atá le bailíochtú agus athmheasúnú leanúnach ar chomhlíonadh tríú páirtí.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – Seirbhísí córais sheachtracha: sainmhínítear ceanglais slándála agus riosca maidir le córais a oibríonn eintitis sheachtracha.

11.3.2 SA-10 – Bainistíocht cumraíochta forbróra: tá feidhm aige nuair a sheachadann tríú páirtithe bogearraí nó timpeallachtaí.

11.3.3 CA-3 – Idirnaisc chórais: ceanglaítear maoirseacht agus comhaontú maidir le sreafaí sonraí córais idir eintitis.

11.3.4 PS-7 – Slándáil pearsanra tríú páirtí: cinntítear go ndéantar scagadh agus faireachán cuí ar chonraitheoirí agus ar fhoireann soláthraithe.

11.4 GDPR an Aontais Eorpaigh (2016/679):

11.4.1 Airteagal 28 – Oibleagáidí próiseálaí: ceanglaítear comhaontuithe i scríbhinn le próiseálaithe sonraí, lena n-áirítear rialuithe teicniúla agus eagraíochtúla (TOManna).

11.4.2 Airteagal 32 – Slándáil na Próiseála: sainordaítear coimircí iomchuí ag rialaitheoirí agus próiseálaithe araon.

11.4.3 Airteagal 33 – Fógra faoi shárú sonraí pearsanta: ceanglaítear fógra pras ó sholáthraithe i gcás sáraithe.

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

11.5.1 Airteagal 21(2)(e–f): ceanglaítear bainistíocht soláthraithe bunaithe ar riosca agus maoirseacht slándála, go háirithe i slabhraí soláthair digiteacha eintitis riachtanacha agus thábhachtacha.

11.6 DORA an Aontais Eorpaigh (2022/2554):

11.6.1 Airteagal 28 – Riosca TFC tríú páirtí: forchuirtear oibleagáidí maidir le measúnú riosca, téarmaí conarthacha slándála agus straitéisí scoir ar sholáthraithe seirbhísí airgeadais.

11.6.2 Airteagal 30 – Maoirseacht ar sholáthraithe criticiúla TFC tríú páirtí: bunaítear ionchais fheabhsaithe faireacháin agus mhaoirseachta i leith príomhsholáthraithe.

11.7 COBIT 2019:

11.7.1 BAI05 – Cumasú athraithe eagraíochtúil a bhainistiú: cinntítear rialachas slán ar aistrithe soláthraithe.

11.7.2 DSS02 – Iarratais seirbhíse agus teagmhais a bhainistiú: tá feidhm aige maidir le saincheisteanna a thuairiscíonn soláthraithe agus le comhtháthú láimhseáil teagmhas.

11.7.3 MEA03 – Faireachán, meastóireacht agus measúnú ar chomhlíonadh: treisítear tomhas feidhmíochta soláthraithe agus faireachán ar chomhlíonadh.