					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P26S					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	Rialuithe oibríochtúla do chaidrimh le tríú páirtithe agus soláthraithe
ISO/IEC 27002:2022	Rialuithe 5.19–5.22	Rialuithe slándála soláthraithe, téarmaí conarthacha slándála, bainistíocht athruithe, faireachán agus athbhreithniú
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Soláthar, cumraíocht, comhaontuithe idirnasctha agus rialuithe maidir le pearsanra seachtrach
GDPR an AE	Airteagail 28, 32	comhaontuithe próiseála sonraí, ceanglais slándála do phróiseálaithe
NIS2 an AE	Airteagail 21(2)(a)(b)(i), 23(1)	bainistíocht riosca sa slabhra soláthair, maoirseacht ar sheirbhísí tríú páirtí
DORA an AE	Airteagail 5(1)(2), 28(1)(2)	bainistíocht riosca TFC do sholáthraithe seirbhíse tríú páirtí
COBIT 2019	APO10, APO12, DSS05	bainistíocht soláthraithe agus comhtháthú riosca

1. Cuspóir

1.1 Bunaítear leis an mbeartas seo na ceanglais éigeantacha slándála maidir le caidrimh le tríú páirtithe agus soláthraithe a bhunú, a bhainistiú agus a fhoirceannadh, i gcás ina bhfaigheann siad rochtain ar shonraí, ar chórais nó ar sheirbhísí na heagraíochta, nó ina mbíonn tionchar acu orthu.

1.2 Cinntíonn sé go láimhseálann soláthraithe seachtracha — lena n-áirítear Soláthraí Tacaíochta TF, oibreoirí seirbhísí scamall, forbróirí bogearraí agus conraitheoirí próiseas gnó — sócmhainní na cuideachta go slán, i gcomhréir leis na dlíthe agus na caighdeáin is infheidhme.

1.3 Laghdaítear leis an mbeartas seo rioscaí amhail sceitheadh sonraí, athruithe neamhúdaraithe ar chórais, fíneálacha rialála, nó cur isteach ar ghnó de dheasca socruithe neamhshlána nó droch-rialaithe le tríú páirtithe.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir le gach tríú páirtí a dhéanann an méid seo a leanas:

2.1.1 Bogearraí, bonneagar, seirbhísí óstála nó seirbhísí scamall a sholáthar

2.1.2 Rochtain a fháil ar chórais, ar ghléasanna nó ar fheidhmchláir inmheánacha, nó iad a bhainistiú

2.1.3 Sonraí, doiciméid nó cúltacaí na cuideachta a láimhseáil

2.1.4 Tacaíocht a sholáthar d'oibríochtaí gnó, AD, airgeadas nó seirbhísí custaiméara

2.2 Tá feidhm aige freisin maidir leis na nithe seo a leanas:

2.2.1 Foireann inmheánach a bhfuil baint aici le soláthraithe a roghnú, a cheapadh nó maoirseacht a dhéanamh orthu

2.2.2 Aon phearsanra a bhainistíonn ionduchtú díoltóirí, conarthaí, rochtain nó athbhreithnithe

2.2.3 Aon chóras nó próiseas atá spleách ar chomhpháirteanna nó ar sheirbhísí tríú páirtí

3. Cuspóirí

3.1 A chinntiú go gcomhlíonann gach soláthraí ionchais slándála atá sainithe go soiléir.

3.2 A cheangal go mbeidh oibleagáidí infhorfheidhmithe slándála, príobháideachais agus freagartha do theagmhais i gconarthaí soláthraithe.

3.3 Rioscaí soláthraithe a mheas agus a dhoiciméadú sula sínítear comhaontuithe nó sula ndeonaítear rochtain.

3.4 Athbhreithnithe rialta a chur i bhfeidhm ar sholáthraithe ardriosca nó criticiúla chun comhlíonadh a dheimhniú.

3.5 Próiseas foirmiúil a bhunú le haghaidh eisceachtaí, bainistíocht teagmhas, agus nuashonruithe conartha.

3.6 Tacú le comhlíonadh oibleagáidí ISO/IEC 27001:2022, GDPR, NIS2 agus DORA a bhaineann le rialachas díoltóirí.

4. Róil agus freagrachtaí

4.1 Bainisteoir Ginearálta (GM)

4.1.1 Tá an chuntasacht dheiridh air as roghnú soláthraithe agus as comhlíonadh slándála

4.1.2 Formheasann sé conarthaí, eisceachtaí agus uaschéimnithe a bhaineann le díoltóirí

4.1.3 Déanann sé maoirseacht ar fhreagairt do theagmhais agus ar chinnteoireacht nuair nach gcomhlíonann díoltóirí a n-oibleagáidí

4.2 Soláthraí TF nó Teagmhálaí Slándála Inmheánach

4.2.1 Déanann sé measúnú ar an rochtain theicniúil a iarrann soláthraithe

4.2.2 Cuireann sé rialuithe rochtana i bhfeidhm, déanann sé athbhreithniú ar logaí, agus fíoraíonn sé láimhseáil shlán sonraí

4.2.3 Déanann sé athbhreithniú ar fhianaise maidir le rialuithe slándála, deimhnithe slándála, nó torthaí iniúchta (nuair is infheidhme)

[... 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 ag an mBainisteoir Ginearálta, le rannpháirtíocht ón Soláthraí TF nó ón mbainisteoir díoltóirí.

9.2 Ní mór athbhreithniú a dhéanamh ar an mbeartas freisin:

9.2.1 Tar éis aon athrú shuntasaigh ar oibleagáidí dlíthiúla, rialála nó conarthacha

9.2.2 Tar éis teagmhas slándála nó fionnachtain iniúchta a bhaineann le soláthraí

9.2.3 Nuair a thugtar isteach catagóirí nua soláthraithe (m.sh. ardáin chriticiúla SaaS)

9.3 Ní mór gach nuashonrú a bheith:

9.3.1 Doiciméadaithe le stair leaganacha agus an réasúnaíocht

9.3.2 Formheasta ag an mBainisteoir Ginearálta

9.3.3 Curtha in iúl don fhoireann inmheánach ábhartha agus do bhainisteoirí soláthraithe

9.3.4 Stóráilte leis na leaganacha roimhe seo de réir P14S – Beartas um Choinneáil Sonraí agus Diúscairt Sonraí

10. Beartais ghaolmhara agus naisc eatarthu

10.1 Braitheann éifeachtacht an bheartais seo ar chomhordú leis na beartais FGBM seo a leanas um shlándáil faisnéise:

10.1.1 P2S – Beartas um Róil agus Freagrachtaí Rialachais: Sanntar ann an chuntasacht as maoirseacht ar sholáthraithe agus as cur chun feidhme conarthaí.

10.1.2 P4S – Beartas Rialaithe Rochtana: Leagtar amach ann rialacha maidir le srianadh rochtana nach mór a chur i bhfeidhm nuair a dheonaítear rochtain ar chórais do sholáthraithe.

10.1.3 P17S – Beartas um Chosaint Sonraí agus Príobháideachas: Cinntítear ann go gcomhlíonann soláthraithe a láimhseálann sonraí pearsanta prionsabail chosanta sonraí agus ceanglais dhlíthiúla.

10.1.4 P14S – Beartas um Choinneáil Sonraí agus Diúscairt Sonraí: Tá feidhm aige maidir le haon sonraí nó taifid a chomhroinntear le soláthraithe nó a stóráiltear acu agus rialaíonn sé diúscairt shlán tar éis fhoirceannadh an chonartha.

10.1.5 P30S – Beartas um Fhreagairt do Theagmhais: Sainmhínítear ann conas freagairt nuair is cúis le teagmhas slándála soláthraí nó nuair a bhíonn baint aige leis, lena n-áirítear nósanna imeachta uaschéimnithe agus láimhseála fianaise.

10.2 Oibríonn na beartais seo le chéile chun a chinntiú go bhfuil riosca soláthraithe faoi rialú ar feadh shaolré an chonartha.

11. Caighdeáin agus creataí tagartha

11.1 ISO/IEC 27001

11.1.1 Clásal 8.1 – Ceanglaíonn sé rialuithe oibríochtúla a chur chun feidhme, lena n-áirítear iad siúd a chuirtear i bhfeidhm ar chaidrimh le tríú páirtithe agus le soláthraithe.

11.2 ISO/IEC 27002

11.2.1 Rialú 5.19 – Cinntíonn sé go bhfuil bearta slándála soláthraithe ailínithe le ceanglais na heagraíochta.

11.2.2 Rialú 5.20 – Ceanglaíonn sé comhaontuithe foirmiúla a chumhdaíonn téarmaí slándála, freagrachtaí agus oibleagáidí sáraithe.

11.2.3 Rialú 5.21 – Rialaíonn sé athruithe ar sheirbhísí soláthraithe a d'fhéadfadh tionchar a imirt ar an staid slándála.

11.2.4 Rialú 5.22 – Ceanglaíonn sé faireachán agus athbhreithniú ar sheirbhísí soláthraithe agus ar chomhlíonadh.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9 – Rialaíonn sé fáil chórais agus seirbhísí seachtracha, agus ceanglaíonn sé measúnuithe riosca agus ionchais shainithe.

11.3.2 SA-10 – Rialaíonn sé nósanna imeachta cumraíochta agus athraithe a bhaineann le córais arna mbainistiú ag tríú páirtithe.

11.3.3 CA-3 – Ceanglaíonn sé comhaontuithe idirnasctha do chórais a bhaineann le heintitis sheachtracha.

11.3.4 PS-7 – Sonraíonn sé scagadh agus cuntasacht maidir le pearsanra seachtrach.

11.4 GDPR an AE (2016/679)

11.4.1 Airteagal 28 – Ceanglaíonn sé comhaontuithe próiseála sonraí le soláthraithe atá ag gníomhú mar phróiseálaithe.

11.4.2 Airteagal 32 – Sainordaíonn sé rialuithe teicniúla agus eagraíochtúla (TOManna) iomchuí do gach próiseálaí sonraí.

11.5 Treoir NIS2 an AE (2022/2555)

11.5.1 Airteagal 21(2)(a), (b), (i) – Sainordaíonn sé bainistíocht riosca i slabhra soláthair TFC agus rialuithe tríú páirtí.

11.5.2 Airteagal 23(1) – Ceanglaíonn sé maoirseacht dhoiciméadaithe ar sheirbhísí tríú páirtí d'eintitis riachtanacha agus thábhachtacha.

11.6 DORA an AE (2022/2554)

11.6.1 Airteagal 5(1) – Ceanglaíonn sé creat bainistíochta riosca TFC a chumhdaíonn gach soláthraí criticiúil tríú páirtí.

11.6.2 Airteagal 5(2) – Forálann sé do rialuithe conarthacha agus oibríochtúla maidir le spleáchais ar sheirbhísí TFC.

11.6.3 Airteagal 28(1), (2) – Bunaíonn sé rialacha maoirseachta do riosca TFC tríú páirtí san earnáil airgeadais.

11.7 COBIT 2019

11.7.1 APO10 – Leagtar amach in "Manage Suppliers" rialuithe foinsithe agus ionchais maidir le bainistíocht caidrimh.

11.7.2 APO12 – Comhtháthaíonn "Manage Risk" riosca soláthraithe i rialachas riosca na heagraíochta.

11.7.3 DSS05 – Tá "Manage Security Services" infheidhme maidir le soláthraithe seirbhísí bainistithe agus soláthraithe seirbhísí seachfhoinsithe tríú páirtí.