					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P40					Teideal an doiciméid: **Beartas um Thástáil Slándála agus Red Teaming**						
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 | 9.1, 9.2, 9.3 |

ISO/IEC 27002:2022 | 5.7, 5.36, 8.8, 8.29, 8.30, 8.1 |

NIST SP 800-53 Rev.5 | CA-2, CA-7, CA-8, RA-5 |

RGCS AE | Airteagal 32(1)(d) |

NIS2 AE | Airteagal 21(2)(f) |

DORA AE | Airteagal 25–27 |

COBIT 2019 | DSS05.07, MEA02.01, MEA02.03 |

1. Cuspóir

1. Sainítear leis an mbeartas seo clár struchtúrtha le haghaidh tástáil rialta slándála ar líonraí, ar chórais agus ar fheidhmchláir na heagraíochta — lena n-áirítear measúnuithe leochaileachta, tástáil treáite agus cleachtaí red team — chun ceanglais Airteagal 21(2)(f) de NIS2 maidir le héifeachtacht beart cibearshlándála a mheas a chomhlíonadh.

1.1 Ní mór a chinntiú go sainaithnítear agus go leigheastar laigí i rialuithe teicniúla agus eagraíochtúla go réamhghníomhach trí thástáil rialaithe, agus ar an gcaoi sin staid slándála na heagraíochta a fheabhsú go leanúnach.

2. Raon feidhme

2. Clúdaíonn an beartas seo gach córas faisnéise criticiúil, feidhmchlár agus bonneagar tacaíochta atá faoi úinéireacht nó á n-oibriú ag an eagraíocht. Áirítear leis freisin tástáil slándála fisiciúla ar shaoráidí a mhéid a bhaineann sí leis an gcibearshlándáil (m.sh. innealtóireacht shóisialta nó tástálacha treáite fisiciúla, má thagann siad faoi raon feidhme red team).

2.1 Tá feidhm ag an mbeartas seo maidir le foirne inmheánacha slándála, le haon ghnólachtaí seachtracha ar conradh a dhéanann tástáil slándála, agus le húinéirí ábhartha córas/feidhmchlár. Ní mór údarú a bheith i bhfeidhm do gach gníomhaíocht tástála agus ní mór na nósanna imeachta sa bheartas seo a leanúint chun cur isteach neamhbheartaithe a sheachaint.

3. Cuspóirí

3. Fíoraítear leis an mbeartas seo éifeachtacht na rialuithe cibearshlándála atá curtha chun feidhme (teicniúil, oibríochtúil agus eagraíochtúil) trí thástáil thréimhsiúil agus insamhaltaí, i gcomhréir le sainordú NIS2 maidir le héifeachtacht a thomhas.

3.1 Aimsítear leochaileachtaí nó bearnaí a d'fhéadfadh gnáthphróisis oibríochtúla a ligean thar ceal, lena n-áirítear saincheisteanna náid-lae nó cumraíochta, faoi chásanna ionsaithe réalaíocha (red teaming) sula mbainfidh naimhde leas astu.

3.2 Cuirtear dearbhú agus moltaí inghníomhaithe ar fáil don bhainistíocht trí thuairisciú ar fhionnachtana na dtástálacha, rud a chuireann ar a cumas cinntí eolasacha a dhéanamh maidir le cóireáil riosca, eisceachtaí agus feabhsú leanúnach ar an gclár slándála.

4. Róil agus freagrachtaí

4. Comhordaitheoir Tástála Slándála (STC): Ceapann an Príomhoifigeach Slándála Faisnéise (CISO) an ról seo, agus tá sé/sí freagrach as gach gníomhaíocht tástála slándála a phleanáil agus a mhaoirsiú. Cinntíonn sé/sí go sainítear raon feidhme na dtástálacha, go n-údaraítear iad, agus go dtuairiscítear agus go gcuirtear na torthaí i ngníomh.

4.1 Foireann Slándála Inmheánach (Blue Team): Comhoibríonn sí sna tástálacha (m.sh. trí fhaisnéis a chur ar fáil chun an raon feidhme a shainiú agus trí fhaireachán a dhéanamh ar chórais le linn na

dtástálacha). I gcás cleachtaí red team, freagraíonn an Blue Team do na hionsaithe ionsamhlaithe, agus déantar measúnú ar a gcumas braite agus freagartha.

4.2 Red Team / Tástálaithe Treáite: D'fhéadfadh gur foireann inmheánach ionsaitheach slándála nó comhairleoirí seachtracha iad. Déanann siad tástálacha faoi rialacha rannpháirtíochta comhaontaithe, déanann siad doiciméadú ar gach leochaileacht agus conair shaothraithe a aimsítear, agus coimeádann siad rúndacht.

[... Níl ailt 4.3–8 san áireamh sa réamhamharc seo. Ceannaigh an doiciméad iomlán chun rochtain a fháil ar an gcomhábhar iomlán. ...]

9. Faireachán agus iniúchadh

9. Ní mór don STC féilire agus loga de gach gníomhaíocht tástála slándála a rinneadh a choinneáil. Ba cheart go n-áireofaí sa loga seo an dáta, an raon feidhme, cé a rinne an tástáil, agus achoimre ar na torthaí. Déanfar athbhreithniú air chun a chinntiú go gcloítear leis an sceideal riachtanach (m.sh. nach bhfágtar aon chóras criticiúil gan tástáil thar an timthriall bliantúil).

9.1 Déanfar faireachán ar dhul chun cinn leigheas na bhfionnachtana tástála agus tuairisceofar air go míosúil. Déanfar athbhreithniú i gcruinnithe bainistíochta ar shaincheisteanna arddéine atá fós gan réiteach go dtí go ndúnfar iad.

9.2 Déanfaidh an fheidhm iniúchta inmheánaigh / an fheidhm chomhlíonta nó iniúchóir neamhspleách athbhreithniú bliantúil ar an gclár tástála slándála lena fhíorú go bhfuil: tástálacha údaraithe, déanta agus tuairiscithe mar is ceart; aghaidh tugtha ar fhionnachtana criticiúla; agus go gcomhlíonann an clár ionchais rialála (mar shampla, d'fhéadfadh iniúchóirí a sheiceáil go ndearnadh tástáil treáite sular seoladh seirbhís nua ar líne, de réir mar is gá). Beidh pleananna gníomhaíochta ceartaitheacha mar thoradh ar aon imeacht.

10. Athbhreithniú agus cothabháil

10. Déanfar athbhreithniú ar an mbeartas seo agus ar an bplean tástála foriomlán ar a laghad uair sa bhliain. Cuirfear san áireamh san athbhreithniú athruithe sa tírdhreach bagairtí (m.sh. teacht chun cinn teicnící ionsaithe nua nach gclúdaíonn ár dtástáil reatha) agus déanfar na raonta feidhme nó na minicíochtaí a oiriúnú dá réir.

10.1 Tar éis aon mhórtheagmhais cibearshlándála nó sáraithe, ní mór athbhreithniú a dhéanamh ar an mbeartas seo chun a chinneadh an bhféadfadh tástáil bhreise nó níos minice an tsaincheist a chosc nó a bhrath. Nuashonrófar an beartas ansin chun na leasuithe sin a ionchorprú (mar shampla, cás nua a chur le cleachtaí red team bunaithe ar phatrúin ionsaithe a breathnaíodh).

10.2 Ní mór don CISO formheas a thabhairt d'aon nuashonrú ar an mbeartas seo agus ní mór é a chur faoi bhráid an Bhoird Bainistíochta. Cuirfear an pearsanra ábhartha ar fad ar an eolas faoi na hathruithe, agus cuirfear comhpháirtithe seachtracha tástála ar an eolas má dhéanann aon athrú difear do théarmaí a rannpháirtíochta.

11. Beartais ghaolmhara agus naisc eatarthu

11.1 P06 – Beartas Bainistíochta Riosca. Cuireann aschuir tástála le measúnú riosca agus le cóireáil riosca.

11.2 P22 – Beartas Logála agus Monatóireachta. Bailíochtaíonn sé clúdach braite le linn cleachtaí.

11.3 P24 – Beartas Forbartha Slána. Comhtháthaíonn sé fionnachtana tástála i rialuithe shaolré forbartha bogearraí (SDLC).

11.4 P25 – Beartas um Cheanglais Slándála Feidhmchlár. Cinntíonn sé go léiríonn na ceanglais na ceachtanna a foghlaimíodh ón tástáil.

11.5 P30 – Beartas Freagartha do Theagmhais. Déanann cásanna red team mionchoigeartú ar playbooks agus ar fhreagairt.

11.6 P31 – Beartas um Bhailiú Fianaise agus Fóiréinsic. Bailíonn sé déantáin le linn tástála go sábháilte.

11.7 P32 – Beartas Leanúnachais Gnó agus Athshlánaithe ó Thubaiste. Fíoraíonn cleachtaí athléimneacht faoi ionsaí.

11.8 P33 – Beartas Faireacháin Iniúchta agus Comhlíonta. Soláthraíonn sé maoirseacht neamhspleách ar éifeachtacht an chláir tástála.

12. Tagairtí

12.1 Treoir NIS2 (AE 2022/2555), Airteagal 21(2), pointe (f) (beartais agus nósanna imeachta chun éifeachtacht beart bainistíochta riosca cibearshlándála a mheas)

12.2 Rialachán Cur Chun Feidhme ón gCoimisiún (AE) 2024/2690, Alt 7 den Iarscríbhinn (ceanglais maidir le faireachán, tástáil agus meastóireacht ar éifeachtacht beart cibearshlándála)

12.3 Treoir Theicniúil ENISA (2025) – Iarscríbhinn ar thástáil slándála agus iniúchadh (treoirlínte maidir le cleachtaí cibearshlándála agus tástálacha teicniúla a dhéanamh)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Dea-Chleachtais Tionscail: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (creataí red teaming don earnáil airgeadais mar thagairt)