					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P25					Teideal an doiciméid: **Beartas um Cheanglais Slándála Feidhmchlár**							
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	—
ISO/IEC 27002:2022	Rialuithe 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
GDPR an AE	Airteagail 25, 32	—
NIS2 an AE	Airteagail 21(2)(f), 23	—
DORA an AE	Airteagail 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Cuspóir

1.1 Sainmhínítear sa bheartas seo ceanglais éigeantacha slándála ar leibhéal an fheidhmchláir maidir le bogearraí a fhorbraíonn, a fhaigheann, a chomhtháthaíonn nó a imscarann an eagraíocht. Cinntíonn sé go ndéantar gach feidhmchlár a dhearadh, a chur chun feidhme agus a chothabháil i gcomhréir le prionsabail na forbartha slána, le hoibleagáidí rialála agus le lamháltas riosca na heagraíochta.

1.2 Leagtar síos sa bheartas seo go gcaithfear slándáil a chomhtháthú ar feadh shaolré iomlán an fheidhmchláir, lena n-áirítear fíordheimhniú úsáideoirí, láimhseáil sonraí, cosaint comhéadain agus idirghníomhaíocht shlán le APIanna nó seirbhísí.

1.3 Tríd an mbeartas seo a ghlacadh, tá sé d'aidhm ag an eagraíocht tabhairt isteach leochaileachtaí bogearraí a chosc, sonraí íogaire a chosaint, agus inrianaitheacht agus athléimneacht in aghaidh saothraithe agus mí-úsáide a chinntiú.

2. Raon feidhme

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

2.1.1 Feidhmchláir a fhorbraítear go hinmheánach nó a fhaightear ó fhoinsí seachtracha, lena n-áirítear SaaS agus uirlisí saincheaptha

2.1.2 Feidhmchláir a thacaíonn le hoibríochtaí gnó criticiúla, le rochtain custaiméirí, nó le próiseáil sonraí rialáilte

2.1.3 Foirne forbartha, DevOps, QA, táirgí agus slándála

2.1.4 Forbróirí tríú páirtí, díoltóirí bogearraí agus comhpháirtithe comhtháthaithe a bhfuil rochtain acu ar fheidhmchláir nó ar APIanna na heagraíochta

2.2 Tá feidhm ag an mbeartas seo i ngach timpeallacht: forbairt, tástáil, stáitsiú, táirgeadh agus athshlánú tubaiste, cibé acu atá siad óstáilte ar an áitreabh, in ionaid sonraí phríobháideacha nó i dtimpeallachtaí scamall poiblí.

3. Cuspóirí

3.1 Sainmhíniú a dhéanamh ar cheanglais bhunúsacha slándála fheidhmiúla agus neamhfheidhmiúla nach mór do gach feidhmchlár a chomhlíonadh, beag beann ar an modh forbartha ná ar an gcruach teicneolaíochta.

3.2 A chinntiú go gcomhtháthaítear cosaintí ar leibhéal an fheidhmchláir, lena n-áirítear bailíochtú ionchuir, ionchódú aschuir, láimhseáil earráidí agus slándáil seisiún.

3.3 A cheangal go gcuirfear meicníochtaí fíordheimhnithe, údaraithe agus rialaithe rochtana chun feidhme go slán agus i gcomhréir le beartais aitheantais agus rochtana na heagraíochta.

3.4 A shainordú go ndéanfar idirghníomhaíocht shlán le APIanna, comhéadain ghréasáin agus comhpháirteanna tríú páirtí trí phrótacail cheadaithe agus rialuithe slándála a úsáid.

3.5 Brath luath agus maolú leochaileachtaí a chumasú trí anailís statach agus dhinimiciúil, athbhreithnithe cód agus samhaltú bagairtí.

3.6 Sonraí íogaire a chosaint i gcomhlíonadh ceanglas rialála trí chriptiú, aicmiú agus loighic coinneála sonraí a fhorfheidhmiú.

3.7 A chinntiú go ndéantar staidiúir slándála feidhmchlár a bhailíochtú go leanúnach tar éis imscartha trí thástáil, faireachán agus ullmhacht iniúchta.

4. Róil agus freagrachtaí

4.1 Príomhoifigeach Slándála Faisnéise (CISO)

4.1.1 Is leis/léi an beartas seo agus cinntíonn sé/sí go bhfuil sé ailínithe le straitéis slándála faisnéise agus le seasamh riosca na heagraíochta.

4.1.2 Formheasann sé/sí ceanglais slándála feidhmchlár agus cinntíonn sé/sí go gcuirtear rialuithe éigeantacha i bhfeidhm ar fud na bhfeidhmeanna forbartha agus soláthair.

4.2 Ceannaire Slándála Feidhmchlár / Bainisteoir DevSecOps

4.2.1 Sainmhíníonn sé/sí rialuithe bunlíne slándála agus modheolaíochtaí tástála do chomhpháirteanna feidhmchláir.

4.2.2 Déanann sé/sí maoirseacht ar chomhtháthú slán uirlisí ar nós SAST, DAST, IAST agus SCA sa phíblíne seachadta bogearraí.

4.2.3 Coinníonn sé/sí an Seicliosta um Cheanglais Slándála Feidhmchlár agus na critéir bhailíochtaithe cothrom le dáta.

[... 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 an beartas seo a athbhreithniú go bliantúil, nó níos minice mar fhreagairt ar na nithe seo a leanas:

9.1.1 Nochtuithe leochaileachta criticiúla a dhéanann difear do chreataí coitianta nó do spleáchais

9.1.2 Nuashonruithe ar oibleagáidí rialála maidir le slándáil feidhmchlár (e.g. NIS2, DORA)

9.1.3 Mórathruithe ar chleachtais forbartha bogearraí, ar uirlisí nó ar ailtireacht scamall na heagraíochta

9.1.4 Fionnachtana ó iniúchtaí inmheánacha nó ó thástálacha treáite seachtracha

9.2 Is é an Ceannaire Slándála Feidhmchlár a stiúrfaidh an t-athbhreithniú, i gcomhordú leis an CISO, le hInnealtóireacht DevOps, leis an bhfeidhm Dlí, le Soláthar agus le ceannairí QA.

9.3 Ní mór gach leasú a chur faoi rialú leaganacha i gClár Rialaithe Doiciméad an ISMS agus a dháileadh ar gach foireann forbartha agus táirgí lena mbaineann.

9.4 Ní mór leaganacha a cuireadh as feidhm a chartlannú ar feadh trí bliana ar a laghad chun tacú le hinrianaitheacht, le hiniúchthacht agus le himscrúduithe sáraithe.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 P1 – Beartas Slándála Faisnéise. Leagtar síos leis seo an bonn chun córais agus sonraí a chosaint, agus faoin mbeartas sin tá gá le rialuithe ar leibhéal an fheidhmchláir chun rochtain neamhúdaraithe, sceitheadh sonraí agus saothrú a chosc.

10.2 P4 – Beartas Rialaithe Rochtana. Sainmhínítear leis seo na caighdeáin maidir le bainistíocht aitheantais agus seisiún nach mór do gach feidhmchlár a fhorfheidhmiú, lena n-áirítear fíordheimhniú láidir, prionsabal na pribhléide is lú agus ceanglais athbhreithnithe rochtana.

10.3 P5 – Beartas um Bainistiú Athruithe. Rialaítear leis seo ardú céime cód feidhmchláir agus cumraíochtaí chuig timpeallachtaí táirgthe, agus cinntítear leis go gcuirtear cosc ar athruithe neamhúdaraithe nó gan tástáil.

10.4 P17 – Beartas um Chosaint Sonraí agus Príobháideachas. Éilítear leis seo ar fheidhmchláir príobháideachas de réir deartha a chur i bhfeidhm agus láimhseáil dhlíthiúil, criptiú agus coinneáil sonraí pearsanta agus íogaire a chinntiú i ngach timpeallacht.

10.5 P24 – Beartas um Fhorbairt Shlán. Soláthraítear leis seo an creat níos leithne chun slándáil a leabú sa SDLC, agus sainmhínítear sa bheartas seo na ceanglais nithiúla agus na rialuithe teicniúla atá le cur chun feidhme laistigh de shraith an fheidhmchláir.

10.6 P30 – Beartas Freagartha do Theagmhais. Sainordaítear leis seo láimhseáil struchtúrtha ar theagmhais slándála feidhmchlár, lena n-áirítear leochaileachtaí a shainaithnítear tar éis imscartha nó le linn tástála treáite, agus leagtar amach leis na nósanna imeachta uaschéimnithe, teorannaithe agus téarnaimh.

11. Caighdeáin agus creataí tagartha

11.1 ISO/IEC 27001:2022

11.1.1 Clásal 8.1 – Pleanáil agus Rialú Oibríochtúil: Éilítear leis go ndéanfar slándáil feidhmchlár a leabú i bpróisis agus i gcórais chun rúndacht, sláine agus infhaighteacht a chinntiú.

11.2 ISO/IEC 27002:2022

11.2.1 Rialuithe 8.25–8.26: Sonraítear leo na hionchais maidir le slándáil ar leibhéal an fheidhmchláir, lena n-áirítear cleachtais chódaithe shlána, samhaltú bagairtí, rialuithe ailtireachta agus bailíochtú bogearraí tríú páirtí.

11.2.2 Rialú 8.25 in Iarscríbhinn A – Saolré Forbartha Slán: Forfheidhmítear leis comhtháthú slándála ar fud shaolré an fheidhmchláir.

11.2.3 Rialú 8.26 in Iarscríbhinn A – Ceanglais Slándála Feidhmchlár: Sainordaítear leis sainmhíniú agus cur chun feidhme rialuithe teicniúla chun feidhmchláir a chosaint ar mhí-úsáid agus ar chomhréiteach.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Tástáil agus Meastóireacht Slándála ag Forbróirí: Sainordaítear leis tástáil statach, dhinimiciúil agus treáite le linn forbartha.

11.3.2 SA-15 – Próiseas Forbartha, Caighdeáin agus Uirlisí: Bunaítear leis caighdeáin fhoirmiúla d'fhorbairt shlán feidhmchlár.

11.3.3 SI-10 – Bailíochtú Ionchuir Faisnéise: Éilítear leis meicníochtaí rialaithe chun ionsaithe insteallta agus parsála a chosc.

11.4 GDPR an AE (2016/679)

11.4.1 Airteagal 25 – Cosaint Sonraí trí Dhearadh agus de réir Réamhshocraithe: Éilítear leis cosaint sonraí agus príobháideachas a chomhtháthú i loighic agus i sreafaí oibre an fheidhmchláir.

11.4.2 Airteagal 32 – Slándáil na Próiseála: Sainordaítear leis bearta teicniúla cuí, amhail bailíochtú ionchuir, criptiú agus rialuithe slána rochtana.

11.5 Treoir NIS2 an AE (2022/2555)

11.5.1 Airteagal 21(2)(f): Éilítear leis láimhseáil leochaileachtaí agus cleachtais shlána do shaolré feidhmchlár i gcás eintitis riachtanacha agus thábhachtacha.

11.5.2 Airteagal 23 – Tuairisciú ar Theagmhais Slándála: Éilítear leis cumais logála agus faireacháin ar leibhéal an fheidhmchláir chun teagmhais shuntasacha a bhrath agus a thuairisciú.

11.6 DORA an AE (2022/2554)

11.6.1 Airteagal 9 – Bainistíocht Riosca TFC: Cuirtear d'oibleagáid ar eintitis airgeadais leis a chinntiú go bhfuil feidhmchláir slán, tástáilte agus athléimneach in aghaidh cibearbhagairtí.

11.6.2 Airteagal 11 – Tástáil Uirlisí TFC: Spreagtar leis tástáil thréimhsiúil treáite agus red teaming ar fheidhmchláir agus ar sheirbhísí criticiúla.

11.7 COBIT 2019

11.7.1 BAI03 – Bainistiú Sainaithint agus Tógáil Réiteach: Bunaítear leis ceanglais deartha agus rialaithe le linn fhorbairt feidhmchlár.

11.7.2 BAI09 – Bainistiú Feidhmchlár: Leagtar béim leis ar chothabháil, faireachán agus feabhsú slán ar fheidhmchláir bheo.

11.7.3 DSS05 – Bainistiú Seirbhísí Slándála: Nascann sé cosaint feidhmchlár le hoibríochtaí agus le rialuithe slándála níos leithne na heagraíochta.