					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P24					Teideal an doiciméid: **Beartas Forbartha Sláine**						
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**

1. Cuspóir

1.1 Sainmhínítear leis an mbeartas seo ceanglais éigeantacha slándála maidir le gníomhaíochtaí forbartha bogearraí agus córas laistigh den eagraíocht, lena n-áirítear tionscadail inmheánacha, forbairt seachfhoinsithe agus comhtháthú cód tríú páirtí.

1.2 Is é an cuspóir slándáil a leabú ar fud Shaolré Forbartha Bogearraí (SDLC) agus a chinntiú go ndéantar leochaileachtaí a shainaithint, a mhaolú agus a chosc sula n-imscartar chuig timpeallacht táirgthe iad.

1.3 Tacaíonn an beartas seo le cur chun feidhme Chlásal 8.1 de ISO/IEC 27001:2022 agus Rialuithe 8.25–8 d'Iarscríbhinn A trí rialachas na forbartha sláine, cleachtais bhailíochtaithe cód agus maoirseacht ar fhorbairt tríú páirtí a chaighdeánú.

2. Raon feidhme

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

2.1.1 Bogearraí, feidhmchláir, scripteanna, comhtháthuithe agus uirlisí uathoibrithe a fhorbraítear go hinmheánach nó go seachtrach

2.1.2 Foirne forbartha, úinéirí táirgí, DevOps, QA, ailtirí, bainisteoirí tionscadail agus conraitheoirí

2.1.3 Timpeallachtaí SDLC, lena n-áirítear córais forbartha, tástála, stáitsithe agus réamhtháirgthe

2.1.4 Comhpháirteanna foinse oscailte agus tríú páirtí a chomhtháthaítear i bhfeidhmchláir inmheánacha

2.1.5 Bogearraí a imscartar ar an láthair, i dtimpeallachtaí scamall príobháideach, hibrideacha nó poiblí

2.2 Tá gach úsáideoir agus eintiteas a ghlacann páirt i bhforbairt, i dtástáil nó in imscaradh córas laistigh de chomhthéacs na heagraíochta faoi réir an bheartais seo, lena n-áirítear Soláthraithe Seirbhíse Bainistithe agus díoltóirí ardáin.

3. Cuspóirí

3.1 Rialuithe slándála a leabú ar fud gach céime d'fhorbairt bogearraí, ón dearadh go dtí an t-imscaradh, chun laghdú riosca réamhghníomhach agus leanúnach a chinntiú.

3.2 Cosaint a dhéanamh ar thabhairt isteach leochaileachtaí inshaothraithe, amhail lochtanna insteallta, fíordheimhniú neamhshlán agus nochtadh do laigí aitheanta tríú páirtí.

3.3 Cleachtais chódaithe shlána a bhunú agus a chur chun feidhme i gcomhréir le OWASP, SANS CWE agus treoirlínte sonracha creata.

3.4 A chinntiú go ndéantar athbhreithniú piaraí, anailís uathoibrithe agus bailíochtú slándála ar gach cód sula ndéantar é a imscaradh.

3.5 Rioscaí forbartha a eascraíonn as gníomhaíochtaí seachfhoinsithe, as cód tríú páirtí a áireamh agus as athúsáid bogearraí foinse oscailte a bhainistiú.

3.6 Timpeallachtaí forbartha, tástála agus stáitsithe a chosaint ar rochtain neamhúdaraithe agus cosc a chur ar úsáid sonraí táirgthe gan mascfháil sonraí nó anaithnidiú ceadaithe.

3.7 Feasacht slándála a chur chun cinn i measc forbróirí, bainisteoirí táirgí agus gairmithe dearbhaithe cáilíochta trí oiliúint rólbhunaithe agus nuashonruithe leanúnacha ar bhagairtí atá ag teacht chun cinn.

4. Róil agus freagrachtaí

4.1 Príomhoifigeach Slándála Faisnéise (CISO)

4.1.1 Is leis/léi an beartas seo agus cinntíonn sé/sí go gcuirtear ceanglais forbartha sláine chun feidhme ar fud na heagraíochta.

4.1.2 Formheasann sé/sí caighdeáin chódaithe shlána agus comhaontuithe forbartha tríú páirtí.

4.1.3 Bailíochtaíonn sé/sí cinntí cóireála riosca maidir le leochaileachtaí gan réiteach nó leochaileachtaí ar cuireadh siar iad.

4.2 Ceannaire Slándála Feidhmchlár / Bainisteoir DevSecOps

4.2.1 Forbraíonn, cothaíonn agus cuireann sé/sí chun cinn treoirlínte códaithe slána.

4.2.2 Comhtháthaíonn sé/sí tástáil shlándála statach agus dhinimiciúil i bpíblínte CI/CD.

4.2.3 Déanann sé/sí athbhreithnithe slándála ar chód agus sainmhíníonn sé/sí bearta leasúcháin éigeantacha.

[... 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 go bliantúil, nó níos minice mar fhreagairt ar:

9.1.1 Mórleasuithe ar mhodheolaíochtaí forbartha nó ar uirlisí DevOps

9.1.2 Teagmhais slándála ábhartha a eascraíonn as leochaileachtaí feidhmchláir

9.1.3 Athruithe ar cheanglais rialála a bhaineann le bogearraí slána (e.g. RGCS, DORA)

9.1.4 Caighdeáin tionscail nua nó faisnéis faoi bhagairtí (e.g. OWASP Top 10, SLSA, MITRE CWE)

9.2 Is é an Ceannaire Slándála Feidhmchlár a stiúrfaidh an t-athbhreithniú beartais i gcomhordú leis an CISO, le hailtirí bogearraí, le ceannaireacht QA agus le comhairle dlí (maidir le himpleachtaí cód tríú páirtí).

9.3 Ní mór aon leasuithe a thaifeadadh i gClár Rialaithe Doiciméad an ISMS, iad a chur faoi rialú leaganacha agus iad a chur in iúl do na foirne lena mbaineann trí nótaí eisiúna nó oiliúint éigeantach.

9.4 Ní mór leaganacha oidhreachta a choinneáil sa stór cartlainne ar mhaithe le hinrianaitheacht dhlíthiúil agus iniúchta.

10. Beartais ghaolmhara agus naisc eatarthu

10.1 P1 – Beartas Slándála Faisnéise. Leagtar síos leis an sainordú straitéiseach chun slándáil a leabú ar fud gach córais faisnéise, agus is rialú oibríochtúil bunúsach inti an fhorbairt shlán.

10.2 P4 – Beartas Rialaithe Rochtana. Sainmhínítear leis na bearta rialaithe chun rochtain ar thimpeallachtaí forbartha, stórtha, uirlisí tógála agus píblínte CI/CD a shrianadh.

10.3 P5 – Beartas um Bainistiú Athraithe. Cinntítear leis go bhfuil athruithe cód, eisiúintí agus imscaradh faoi réir formheasa cuí, pleanála rollta siar agus fíoraithe iar-imscartha.

10.4 P12 – Beartas Bainistíochta Sócmhainní. Tacaíonn sé le fardal timpeallachtaí forbartha, stórtha foinse agus córais tógála mar shócmhainní bainistithe atá faoi réir aicmithe agus cosanta.

10.5 P22 – Beartas Logála agus Monatóireachta. Baineann sé le píblínte forbartha agus cinntíonn sé go ndéantar próisis tógála, cur chun cinn cód agus imeachtaí imscartha a logáil, a fhaireachán agus a anailísiú le haghaidh neamhrialtachtaí slándála.

10.6 P30 – Beartas Freagartha do Theagmhais. Soláthraítear leis an gcreat chun lochtanna slándála a aimsítear tar éis imscartha nó le linn tástála slándála feidhmchlár a anailísiú agus freagairt dóibh.

11. Caighdeáin agus creataí tagartha

11.1 ISO/IEC 27001

11.1.1 Clásal 8.1 – Pleanáil agus rialú oibríochtúil: Éilítear leis próisis agus rialuithe forbartha sláine a chomhtháthú in oibríochtaí.

11.2 ISO/IEC 27002:2022 – Rialuithe 8.25–8

11.2.1 Rialú 8.25 d'Iarscríbhinn A – Saolré Forbartha Sláine: Forfheidhmítear cuimsiú foirmiúil slándála i ndearadh agus i bhforbairt bogearraí.

11.2.2 Rialú 8.26 d'Iarscríbhinn A – Ceanglais Slándála Feidhmchlár: Éilítear sainmhíniú ar chódú slán agus ar chritéir ghlactha slándála.

11.2.3 Rialú 8.27 d’Iarscríbhinn A – Ailtireacht Shlán Córas agus Prionsabail Innealtóireachta: Éilítear cur i bhfeidhm prionsabal deartha slándála agus maolú ar laigí aitheanta.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 go SA-15: Bunaítear cleachtais struchtúrtha forbartha slándála feidhmchlár, lena n-áirítear ceanglais maidir le dearadh, sláine cód agus tástáil.

11.3.2 SI-10 – Bailíochtú ionchuir faisnéise: Tugtar aghaidh leis ar chosaintí códaithe slána.

11.3.3 SR-3 – Cosaint an tslabhra soláthair: Éilítear grinnfhiosrú ar bhogearraí, ar chomhpháirteanna agus ar sholáthraithe forbartha tríú páirtí.

11.4 RGCS an Aontais Eorpaigh (2016/679)

11.4.1 Airteagal 25 – Cosaint sonraí trí dhearadh agus mar réamhshocrú: Forordaítear slándáil agus príobháideachas a leabú i bhforbairt córas.

11.4.2 Airteagal 32 – Slándáil na próiseála: Tacaítear leis bearta teicniúla amhail bailíochtú ionchuir, rialuithe rochtana agus imscaradh slán.

11.5 Treoir NIS2 an Aontais Eorpaigh (2022/2555)

11.5.1 Airteagal 21(2)(e–f): Éilítear cleachtais forbartha bogearraí, lena n-áirítear bainistiú leochaileachtaí, slándáil cód agus tuairisciú teagmhas.

11.6 DORA an Aontais Eorpaigh (2022/2554)

11.6.1 Airteagal 9 – Bainistiú riosca TFC: Éilítear cleachtais forbartha sláine d’eintitis airgeadais, lena n-áirítear rialuithe cáilíochta bogearraí agus leasú lochtanna.

11.6.2 Airteagal 10 – Leanúnachas gnó agus tástáil: Spreagtar leis tástáil agus bailíochtú dian ar chórais TFC, lena n-áirítear feidhmchláir.

11.7 COBIT 2019

11.7.1 BAI03 – Bainistiú Sainaithint Réiteach agus Tógáil: Rialaítear leis dearadh, forbairt agus comhtháthú slándála i réitigh nua.

11.7.2 BAI07 – Bainistiú Glacadh le hAthrú agus Aistriú: Cinntítear leis imscaradh slán agus meastóireacht iar-imscartha.

11.7.3 DSS05 – Bainistiú Seirbhísí Slándála: Cuirtear bailíochtú slándála i bhfeidhm ar sholáthar bogearraí agus seirbhísí.