					Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe						
Uimhir an doiciméid: P11					Teideal an doiciméid: **Beartas um Bainistíocht Cuntas Úsáideora agus Pribhléidí**						
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 6.1.3, Clásal 8	-
ISO/IEC 27002:2022	Rialuithe 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2-IA-5, AU-2, AU-12	-
GDPR an Aontais Eorpaigh	Airteagail 5(1)(f), 32; Aithris 39	-
NIS2 an Aontais Eorpaigh	Airteagail 21(2)(a, d), 21(3)	-
DORA an Aontais Eorpaigh	Airteagail 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Cuspóir

1 Bunaítear leis an mbeartas seo rialuithe éigeantacha maidir le bainistíocht cuntas úsáideora agus pribhléidí ar fud gach córais faisnéise agus seirbhíse. Cinntítear leis go ndeonaítear rochtain ar acmhainní na heagraíochta ar bhonn aitheantais bhailíochtaithe, riachtanas róil, agus phrionsabail na pribhléide íosta agus scaradh dualgas.

1.1 Tacaíonn sé le tiomantas na heagraíochta do shlándáil faisnéise trí phróisis struchtúrtha, ininiúchta a chur chun feidhme le haghaidh soláthar rochtana, sannadh pribhléidí, faireachán ar úsáid, agus cúlghairm rochtana.

1.2 Tá an beartas seo ríthábhachtach chun an riosca a bhaineann le rochtain neamhúdaraithe, mí-úsáid pribhléidí, bagairtí ón taobh istigh, agus neamhchomhlíonadh na gcreataí rialála is infheidhme a laghdú.

2. Raon feidhme

2.1 Tá feidhm ag an mbeartas seo maidir le gach fostaí, conraitheoir, soláthraí seirbhíse tríú páirtí, comhairleoir, agus daoine eile a fhaigheann rochtain ar acmhainní TF, feidhmchláir nó sonraí na heagraíochta.

2.2 Rialaíonn sé gach córas agus timpeallacht ina gcuirtear meicníochtaí fíordheimhnithe úsáideora agus rialaithe rochtana i bhfeidhm, lena n-áirítear, ach gan a bheith teoranta do:

2.2.1 Feidhmchláir fhiontair agus bunachair shonraí

2.2.2 Ardáin scamallbhunaithe agus timpeallachtaí SaaS

2.2.3 Córais oibriúcháin agus consóil riaracháin

2.2.4 Uirlisí cianrochtana agus VPNanna

2.2.5 Córais bainistíochta aitheantais agus rochtana (IAM)

2.3 Cuimsíonn an beartas seo cuntais úsáideora chaighdeánacha agus cuntais úsáideora phribhléideacha araon, agus áirítear leis rialuithe ar:

2.3.1 Cruthú, modhnú agus díghníomhachtú cuntas

2.3.2 Uaschéimniú pribhléidí agus tarmligean

2.3.3 Rialú agus faireachán seisiún

2.3.4 Modhanna fíordheimhnithe agus bainistíocht dintiúr

3. Cuspóirí

3.1 A chinntiú go bhfuil gach cuntas úsáideora inaitheanta go huathúil, údaraithe i gceart, agus sannta ach amháin tar éis bailíochtú foirmiúil ar riachtanas.

3.2 Prionsabal na pribhléide íosta a chur i bhfeidhm agus rochtain neamhriachtanach nó iomarcach a chosc trí rialuithe dochta ar eisiúint agus úsáid cuntas pribhléideach a fhorfheidhmiú.

3.3 A cheangal go ndéanfar stádas cuntais a nuashonrú in am bunaithe ar athruithe fostaíochta nó róil, lena n-áirítear díghníomhachtú láithreach ar fhoirceannadh.

3.4 Brath agus leasú réamhghníomhach ar chuntais neamhghníomhacha, mhí-úsáidte nó neamhúdaraithe a chumasú trí logáil, athbhreithnithe, agus uathoibriú.

3.5 Ailíniú le ISO/IEC 27001:2022 agus le caighdeáin ghaolmhara a choinneáil, agus oibleagáidí faoi chreataí dlíthiúla agus rialála ábhartha amhail GDPR, NIS2, DORA, agus COBIT 2019 a chomhlíonadh.

4. Róil agus freagrachtaí

4.1 Príomhoifigeach Slándála Faisnéise (CISO)

4.1.1 Is leis an ról seo an beartas seo agus cinntíonn sé a chur chun feidhme ar fud na heagraíochta.

4.1.2 Déanann sé athbhreithniú ar aon eisceachtaí foirmiúla nó cásanna rochtana éigeandála agus formheasann sé iad.

4.1.3 Tuairiscíonn sé torthaí iniúchta a bhaineann le cuntais agus ardaíonn sé rioscaí chuig an mBainistíocht Feidhmiúcháin.

4.2 Bainisteoir Rialaithe Rochtana / Riarthóir TF

4.2.1 Coinníonn agus oibríonn sé na rialuithe teicniúla do bhainistíocht shaolré cuntas úsáideora.

4.2.2 Déanann sé soláthar rochtana, dísholáthar rochtana, agus gníomhaíochtaí bainistíochta pribhléidí ar bhonn iarratas ceadaithe.

4.2.3 Coinníonn sé clár údarásach de gach cuntas úsáideora, a stádas, agus a leibhéal pribhléide.

4.2.4 Tacaíonn sé le hiniúchtaí agus le hathbhreithnithe comhlíonta trí logaí agus tuarascálacha gníomhaíochta a chur ar fáil.

[... 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 Déanfar athbhreithniú ar an mbeartas seo ar a laghad uair sa bhliain nó tráth a tharlóidh athruithe suntasacha ar:

9.1.1 Struchtúr eagraíochtúil nó próisis ghnó

9.1.2 Córais TF, ardáin aitheantais, nó modhanna rochtana

9.1.3 Ceanglais rialála nó chonarthacha a bhaineann le bainistíocht aitheantais agus rochtana

9.2 Beidh an Príomhoifigeach Slándála Faisnéise (CISO), i gcomhar leis an mBainisteoir Rialaithe Rochtana, freagrach as an bpróiseas athbhreithnithe a thionscnamh agus as aiseolas ó pháirtithe leasmhara a chomhordú.

9.3 Féadfar athbhreithnithe eatramhacha a spreagadh le:

9.3.1 Teagmhais slándála a bhaineann le mí-úsáid cuntas

9.3.2 Torthaí iniúchta a tharraingíonn aird ar easnaimh i mbainistíocht shaolré cuntas

9.3.3 Imscaradh uirlisí nua bainistíochta aitheantais nó bainistíochta rochtana pribhléidí

9.4 Ní mór nuashonruithe ar an mbeartas seo a bheith:

9.4.1 Faoi rialú leaganacha agus taifeadta i leabharlann doiciméadachta an ISMS

9.4.2 Curtha in iúl do gach páirtí leasmhar ábhartha, lena n-áirítear Cinn Roinne, oibríochtaí TF, agus AD

9.4.3 Tacaithe ag ábhair oiliúna nuashonraithe agus treoracha nós imeachta

9.5 Ní mór gach athrú a bheith ceadaithe ag an mBainistíocht Feidhmiúcháin nó ag an gCoiste Stiúrtha Slándála Faisnéise (ISSC) agus a logáil chun críocha iniúchta.

10. Beartais ghaolmhara agus nascachtaí

10.1 Tá an beartas seo nasctha go hoibríochtúil leis na beartais ghaolmhara seo a leanas laistigh de shraith an ISMS agus tacaítear leis acu:

10.1.1 P4 Beartas Rialaithe Rochtana: Bunaítear leis na prionsabail agus na meicníochtaí foriomlána rialaithe rochtana, lena n-áirítear rialuithe riailbhunaithe agus rialuithe rólbhunaithe.

10.1.2 P7 Beartas Ionduchtaithe agus Foirceanta: Soláthraítear leis céimeanna nós imeachta chun rochtain úsáideora a thionscnamh agus a fhoirceannadh i gcomhréir le gníomhartha AD.

10.1.3 P8 Beartas Feasachta agus Oiliúna um Shlándáil Faisnéise: Neartaítear leis freagrachtaí úsáideoirí maidir le slándáil cuntas agus cosaint dintiúr.

10.1.4 P13 Beartas Aicmithe agus Lipéadaithe Sonraí: Treoraítear leis leibhéil rochtana bunaithe ar aicmiú sonraí, chun a chinntiú go bhfuil teorainneacha pribhléidí ailínithe le sraitheanna íogaireachta.

10.1.5 P22 Beartas Logála agus Monatóireachta: Cinntítear leis go mbailítear rianta iniúchta do gach gníomhaíocht a bhaineann le cuntais agus go ndéantar athbhreithniú orthu chun neamhrialtachtaí nó úsáid neamhúdaraithe a bhrath.

10.1.6 P30 Beartas Freagartha do Theagmhais: Rialaítear leis ardú céime, teorannú, agus gníomhartha iartheagmhais i gcásanna mí-úsáide pribhléidí nó gníomhaíochta cuntais neamhúdaraithe.

10.2 Oibríonn gach ceann de na beartais seo i gcomhar lena chéile chun creat comhleanúnach, rioscabhunaithe a fhorfheidhmiú maidir le bainistíocht aitheantais agus rochtana ar fud na heagraíochta.

11. Caighdeáin agus creataí tagartha

11.1 Tá an beartas seo ailínithe le caighdeáin chibearshlándála agus le creataí rialála a aithnítear go hidirnáisiúnta, lena gceanglaítear bainistíocht shlán aitheantais, rochtana, agus pribhléidí mar chroíchuid de shlándáil faisnéise eagraíochtúil.

11.2 ISO/IEC 27001:

11.2.1 Clásal 6.1.3 - ceanglaítear ar eagraíochtaí rioscaí slándála faisnéise a shainaithint, a mheasúnú, agus a chóireáil, rud a fhágann gur rialú foirmiúil rioscabhunaithe é bainistíocht rochtana agus pribhléidí atá leabaithe i bpróiseas pleanála an ISMS.

11.2.2 Clásal 8.1 - Pleanáil agus Rialú Oibríochtúil: Treisíonn sé cur i bhfeidhm coimircí teicniúla agus nós imeachta a rialaíonn rochtain úsáideora agus rochtain phribhléideach.

11.3 ISO/IEC 27002:2022 - Rialuithe 5.15 go 5.18:

11.3.1 Rialú 5.15 - Bainistíocht Rochtana Úsáideora: Tacaíonn sé le próisis fhoirmiúla maidir le soláthar rochtana, údarú rochtana, agus athbhreithniú tréimhsiúil ar chearta rochtana.

11.3.2 Rialú 5.16 - Bainistíocht Aitheantais: Bunaíonn sé uathúlacht aitheantais, rialuithe saolré, agus forfheidhmiú fíordheimhnithe shlána.

11.3.3 Rialú 5.17 - Faisnéis Fhíordheimhnithe: Cinntíonn sé go ndéantar leithdháileadh agus úsáid faisnéise fíordheimhnithe a rialú go docht, a dhéanamh inrianaithe, agus a ailíniú le prionsabal na pribhléide íosta ar feadh shaolré an chuntais úsáideora.

11.3.4 Rialú 5.18 - Cearta Rochtana: Tugtar aghaidh iomlán air trí shannadh pribhléidí rólbhunaithe, iniúchóireacht, agus ceanglais cheadaithe le haghaidh rochtain ardaithe.

11.4 Treoraíonn na rialuithe seo cur chun feidhme struchtúrtha ar chlárú cuntas, díchlárú, scaradh pribhléidí, agus úsáid faisnéise fíordheimhnithe. Forfheidhmíonn an beartas rialachas shaolré

aitheantais, rochtain díreach in am, agus faireachán ar sheisiúin ardaithe chun úsáid neamhúdaraithe córais a chosc.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Beartas Rialaithe Rochtana) agus AC-2 (Bainistíocht Cuntas): Mapáiltear iad trí shainorduithe beartais maidir le ceaduithe rochtana, mapáil ról, agus iniúchóireacht cuntas úsáideora.

11.5.2 AC-5 (Scaradh dualgas) agus AC-6 (prionsabal na pribhléide íosta): Comhlíontar iad trí shrianadh pribhléidí, ailíniú le róil poist, agus décheadú do thascanna ardriosca.

11.5.3 IA-2 go IA-5 (Aithint agus Fíordheimhniú): Forfheidhmítear iad trí mheicníochtaí láidre fíordheimhnithe, rialacha shaolré dintiúr, agus ceanglais MFA.

11.5.4 AU-2, AU-12 (Logáil iniúchta agus anailís): Tugtar aghaidh orthu trí thaifeadadh seisiún agus faireachán ar ghníomhaíocht phribhléideach ar fud timpeallachtaí íogaire.

11.6 GDPR an Aontais Eorpaigh (2016/679):

11.6.1 Airteagal 32 - Slándáil na Próiseála: Éilíonn sé rialuithe rochtana agus meicníochtaí fíoraithe aitheantais chun sonraí pearsanta a chosaint. Comhlíontar é trí cheaduithe cuntas, athbhreithnithe pribhléidí, agus coimircí láidre fíordheimhnithe a shainordú.

11.6.2 Airteagal 5(1)(f) - Sláine agus Rúndacht: Cinntíonn sé nach mbíonn rochtain ar shonraí pearsanta ach ag úsáideoirí údaraithe a bhfuil róil dhlisteanacha acu, agus é sin treisithe trí chur chun feidhme bainistíochta cuntas.

11.6.3 Aithris 39: Iarrann sí teorannú soiléir rochtana agus cuntasacht — tacaíonn an beartas seo le hinrianaitheacht iomlán ar aitheantais úsáideoirí agus ar shannadh pribhléidí.

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

11.7.1 Airteagal 21(2)(a, d): Éilíonn sé ar eintitis beartais bainistíochta rochtana a fhorfheidhmiú agus láimhseáil shlán dintiúr agus seisiún pribhléideach a chinntiú, le tacaíocht ó rialuithe an bheartais seo maidir le soláthar, faireachán, agus eisceachtaí.

11.7.2 Airteagal 21(3): Cuireann sé smacht rochtana agus dearbhú láidir aitheantais chun cinn in earnálacha criticiúla, agus baintear é sin amach trí úsáid a bhaint as aitheantóirí uathúla, RBAC, agus rochtain ardaithe faoi shrian ama.

11.8 DORA an Aontais Eorpaigh (2022/2554):

11.8.1 Airteagal 5 - Rialachas agus Rialú TFC: Sainordaíonn sé próisis fhoirmiúla le haghaidh bainistíocht úsáideoirí TFC, a chumhdaítear trí nósanna imeachta doiciméadaithe maidir le soláthar, díghníomhachtú, agus láimhseáil eisceachtaí.

11.8.2 Airteagal 9 - Bainistiú Riosca TFC: Treoraíonn sé eagraíochtaí chun córais a dhaingniú trí shrianta rochtana agus faireachán, agus tugtar aghaidh air sin trí MFA, logáil rochtana pribhléidí, agus athbhreithnithe láraithe.

11.9 COBIT 2019:

11.9.1 DSS01 - Oibríochtaí Bainistithe: Cuireann sé cur i bhfeidhm rialuithe oibríochtúla caighdeánaithe chun cinn, lena n-áirítear bainistíocht shaolré cuntas úsáideora agus doiciméadacht rochtana.

11.9.2 DSS05 - Seirbhísí Slándála Bainistithe: Léiríonn sé riar slán ar phribhléidí úsáideora agus córais, ag tacú le maolú riosca trí phribhléid íosta agus bailíochtú rian iniúchta.

11.9.3 APO13 - Slándáil Bhainistithe: Éilíonn sé rialachas rochtana ar fud sócmhainní digiteacha, a chomhlíontar trí chleachtais fhoirmiúla maidir le húdarú cuntas agus ról, mar aon le sainorduithe athbhreithnithe tréimhsiúla.