

				Cuir isteach anseo ainm an eintitis dhlíthiúil chláraithe							
Uimhir an doiciméid: P11S				Teideal an doiciméid: Beartas um Bainistíocht Cuntas Úsáideoirí 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	Athbhreithnithe ag	Úinéir an phróisis

Formheasanna			
Ainm	Post	Dáta	Síniú

Fógra dlíthiúil (cóipcheart agus srianta úsáide)
(C) 2025 Clarysec LLC. All rights reserved.

Is maoin intleachtúil de chuid Clarysec LLC an doiciméad seo. Ní ceadmhach aon chuid den doiciméad seo a chóipeáil, a athúsáid, a dháileadh ná a mhodhnú chun críocha tráchtála ná cur chun feidhme gan cead sainráite i scríbhinn roimh ré.

Tá úsáid neamhúdaráithe toirmisce go dian agus d'fhéadfadh caingeán dlíthiúil a bheith mar thoradh uirthi. Le haghaidh ceadúnaithe, déan teagmháil le: info@clarysec.com

Ailínithe le caighdeáin agus rialacháin

Caighdeán/Rialachán	Clásal/Airteagal	Nóta
ISO/IEC 27001:2022	Clásail 5.3, 8	Róil, freagrachtaí agus pleanáil/rialú oibríochtúil do bhainistíocht rochtana úsáideoirí
ISO/IEC 27002:2022	Rialú 8	Rialuithe chun pribhléidí ardaithe a shannadh, a athbhreithniú agus a bhaint
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Cruthú cuntas, faireachán, prionsabal na pribhléide is lú agus scaradh dualgas
EU NIS2	Airteagal 21(2)(d)	Bainistíocht rochtana úsáideoirí d'eintitis riachtanacha agus thábhachtacha
EU DORA	Airteagal 9(2)(b)	Rialú rochtana pribhléidí in eintitis airgeadais
COBIT 2019	DSS05.03, DSS05.04	Soláthar rochtana, baint rochtana agus athbhreithniú tréimhsiúil ar rochtain úsáideoirí
EU GDPR	Airteagal 32	Rialuithe rochtana iomchuí chun sonraí pearsanta a chosaint

1. Cuspóir

1.1 Leagtar síos sa bheartas seo na rialacha chun cuntais úsáideoirí agus cearta rochtana a bhainistiú ar bhealach slán, comhsheasmhach agus inrianaithe. Cinntítear leis nach mbeidh rochtain ar chórais ná ar shonraí ach ag úsáideoirí údaraithe, agus go mbeidh an rochtain sin iomchuí dá ról agus dá bhfreagrachtaí.

1.2 Tá bainistíocht éifeachtach cuntas agus pribhléidí riachtanach chun rochtain neamhúdaraithé a chosc, bagairtí inmheánacha a íoslaghú, agus comhlíonadh le ISO/IEC 27001, GDPR agus ceanglais rialála eile a chinntiú.

1.3 Cumasaíonn an beartas seo don eagraíocht úinéireacht agus freagracht a shannadh maidir le húsáid cuntas, faireachán agus iniúchadh a dhéanamh ar ardú pribhléidí, agus rochtain a dhíchumasú nó a chúlghairm go slán nuair nach mbíonn sí de dhíth a thuilleadh.

1.4 Cosnaíonn sé freisin oibríochtaí gnó ar earráidí oibríochtúla nó ar mhí-úsáid de dheasca rochtana iomarcaí nó rochtana nach bhfuil faoi faireachán, agus cuidíonn sé leis an riosca a bhaineann le sceitheadh sonraí de thaisme, mí-úsáid pribhléidí nó neamhchomhlíonadh rialála a laghdú.

2. Raon feidhme

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

2.1.1 Gach fostaí, intéirneach, conraitheoir agus úsáideoir tríú páirtí a bhfuil rochtain acu ar chórais TF na heagraíochta

2.1.2 Gach córas, gléas, seirbhís agus ardán a bhainistíonn an eagraíocht nó a bhainistítear thar a ceann, lena n-áirítear ardáin scamallbhunaithe, bonneagar ar an áitreabh agus uirlisí tríú páirtí

2.2 Cumhdaíonn sé gach cineál cuntas úsáideoira, lena n-áirítear:

2.2.1 Cuntais úsáideoira ainmnithe (m.sh. cuntais ríomhphoist, logálacha isteach córais)

2.2.2 Cuntais riarthóra agus cuntais ar leibhéal an chórais

2.2.3 Dintiúir rochtana sealadacha, aíochta nó tríú páirtí

2.2.4 Cuntais seirbhíse a úsáideann feidhmchláir nó córais uathobrithe

2.3 Tá feidhm ag an mbeartas seo ar feadh shaolré iomlán an chuntais — ón gcruthú agus an formheas go dtí an modhnú, an faireachán agus an díghníomhachtú. Áirítear leis sin an soláthar tosaigh le linn ionduchtaithe, athbhreithnithe rochtana le linn athruithe róil, agus cúlghairm le linn eisduchtaithe.

3. Cuspóirí

3.1 Aitheantais úsáideora uathúla agus inrianaithe a shannadh do gach úsáideoir córais chun cuntasacht a chinntiú agus deireadh a chur le spleáchas ar dhintiúir chomhroinnte.

3.2 Prionsabal na pribhléide is lú a chur i bhfeidhm, ionas nach dtabharfar d'úsáideoirí ach an leibhéal íosta rochtana is gá chun a ndualgais a chomhlíonadh.

3.3 Rochtain neamhúdaraithé ar chórais nó ar shonraí íogaire a chosc trí phróisis formheasa agus athbhreithnithe atá doiciméadaithe go soiléir.

3.4 Díghníomhachtú tráthúil cuntas úsáideora a chinntiú nuair nach mbíonn siad riachtanach a thuilleadh — m.sh. tráth foirceanta, chríochnú conartha nó athruithe róil.

3.5 Timpeallacht shlán a chothabháil a thacaíonn le hullmhacht iniúchta trí gach athrú cuntais, formheas agus athbhreithniú tréimhsiúil a dhoiciméadú.

3.6 A chinntiú go ndéantar ardú pribhléidí a rialú go docht, a fhaomhadh go neamhspleách agus a logáil, agus go mbaintear rochtain ardaithé go pras nuair nach mbíonn gá léi a thuilleadh.

4. Róil agus freagrachtaí

4.1 Bainisteoir Ginearálta (GM)

4.1.1 Tá an chuntasacht fhoriomlán air/uirthi as cur chun feidhme an bheartais seo.

4.1.2 Cinntíonn sé/sí go bhfuil cleachtais bhainistíochta cuntas ailínithe le ceanglais deimhniúcháin ISO/IEC 27001 agus le hoibleagáidí dlí ábhartha (m.sh. GDPR).

4.1.3 Ní mór aon rochtain neamhúdaraithé, teagmhas slándála nó sárú beartais a bhaineann le cuntais úsáideoirí a chur in iúl dó/di láithreach.

4.1.4 Déanann sé/sí maoirseacht ar athbhreithnithe beartais, ar iniúchtaí agus ar ghníomhartha cur chun feidhme.

4.2 Ceannaire TF nó Soláthraí Seirbhísí TF Seachtrach

4.2.1 Tá sé/sí freagrach as rialuithe cuntas agus pribhléidí a chur i bhfeidhm go teicniúil ar fud na gcóras a úsáideann an eagraíocht.

4.2.2 Ní mór dó/di cuntais úsáideoirí a sholáthar, a mhodhnú agus a dhíghníomhachtú ar bhonn formheasanna doiciméadaithe amháin.

4.2.3 Ní mór dó/di castacht pasfhocal, teorainn ama scáileáin, fíordheimhniú ilfhachtóiriúil (MFA) (más ar fáil), agus logáil chórais a chur i bhfeidhm.

4.2.4 Ní mór dó/di taifid shlána a choinneáil ar gach formheas rochtana, úinéireacht cuntas, ardú pribhléidí agus cúlghairm.

4.2.5 Ceanglaítear air/uirthi faireachán a dhéanamh ar chuntais neamhúdaraithé nó cuntais dhílleachtacha agus neamhréireachtaí a thuairisciú don GM.

[... 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 don GM agus don Ceannaire TF athbhreithniú a dhéanamh ar an mbeartas seo uair sa bhliain ar a laghad chun comhlíonadh leis na nithe seo a leanas a chinntiú:

- 9.1.1 Rialuithe agus treoir reatha ISO/IEC 27001:2022
- 9.1.2 Nuashonruithe rialála (m.sh. GDPR, DORA, NIS2)
- 9.1.3 Athruithe i gcórais, i seirbhísí nó i struchtúr gnó

9.2 Ní mór athbhreithnithe a dhéanamh freisin tar éis:

- 9.2.1 Teagmhais slándála shuntasacha nó fionnachtana iniúchta
- 9.2.2 Mórathruithe i gcórais TF nó in ailtireacht cuntas
- 9.2.3 Ardáin nua a thabhairt isteach a éilíonn comhtháthú rialaithe rochtana

9.3 Ní mór don GM gach athrú a fhaomhadh agus iad a chur in iúl go soiléir don fhoireann lena mbaineann.

10. Beartais ghaolmhara agus naisc eatarthu

- 10.1 P2S – Beartas um Róil agus Freagrachtaí Rialachais: Bunaítear leis cuntasacht agus údarás cinnteoireachta maidir le formheasanna rochtana agus maoirseacht.
- 10.2 P4S – Beartas Rialaithe Rochtana: Rialaíonn sé cur chun feidhme rialuithe rochtana ar fud an chórais agus modhanna fíordheimhnithe.
- 10.3 P7S – Beartas Ionduchtaithe agus Foirceanta: Cinntíonn sé go bhfuil cruthú agus baint cuntas leabaithe sna hathruithe pearsanra a bhainistíonn AD.
- 10.4 P8S – Beartas Feasachta agus Oiliúna um Shlándáil Faisnéise: Soláthraíonn sé oiliúint d'úsáideoirí maidir le cleachtais shlána cuntas agus ionchais úsáide.
- 10.5 P30S – Beartas um Fhreagairt do Theagmhais: Sainmhíníonn sé na gníomhartha atá le déanamh má bhíonn sárú slándála nó nochtadh neamhúdaraíthe mar thoradh ar mhí-úsáid cuntais.

11. Caighdeáin agus creataí tagartha

11.1 ISO/IEC 27001

- 11.1.1 Clásal 5.3: Ceanglaítear go sannfar agus go gcuirfear i bhfeidhm go soiléir róil agus freagrachtaí maidir le slándáil faisnéise.
- 11.1.2 Clásal 8.1: Ní mór bainistíocht rochtana úsáideoirí a áireamh i bpleanáil agus i rialú oibríochtúil.

11.2 ISO/IEC 27002

- 11.2.1 Rialú 8.2: Leagtar amach rialuithe teicniúla agus nós imeachta chun pribhléidí ardaithe a shannadh, a athbhreithniú agus a bhaint.

11.3 NIST SP 800-53 Rev.5

- 11.3.1 AC-2: Ceanglaítear cruthú cuntas, faireachán agus cúlghairm bunaithe ar róil agus ar phróisis shainithe.
- 11.3.2 AC-5: Tugtar aghaidh ar scaradh dualgas chun coinbhleacht nó mí-úsáid pribhléidí a chosc.
- 11.3.3 AC-6: Sainordaítear cur i bhfeidhm phrionsabal na pribhléide is lú maidir le gach ceart rochtana.

11.4 EU GDPR

- 11.4.1 Airteagal 32: Ceanglaítear rialuithe rochtana iomchuí chun sonraí pearsanta a chosaint ar rochtain neamhúdaraíthe nó ar athrú neamhúdaraíthe.

11.5 EU NIS

- 11.5.1 Airteagal 21(2)(d): Sainordaítear bainistíocht rochtana úsáideoirí mar chuid de na príomhrialuithe slándála d'eintitis riachtanacha agus thábhachtacha.

11.6 EU DORA

- 11.6.1 Airteagal 9(2)(b): Ceanglaítear ar eintitis airgeadais rialuithe rochtana a chur i bhfeidhm a chuireann srian ar chearta pribhléideacha agus a dhéanann faireachán orthu.

11.7 COBIT 2019

11.7.1 DSS05.03: Sonraítear soláthar rochtana agus baint rochtana úsáideoirí mar chuid de rialachas TF.

11.7.2 DSS05.04: Éilítear athbhreithniú leanúnach agus ailíniú rochtana úsáideoirí le ról eagraíochtúla.