Polisi Cyfrineiriau Systemau TG Prifysgol Caerdydd

Rhif y Fersiwn	1.3
Statws y Ddogfen	Cymeradwywyd
Dyddiad cymeradwyo	15 Ionawr 2019
Cymeradwywyd Gan	Grŵp Goruchwylio Rheoli Data a Gwybodaeth
Dyddiad Dod i Rym	15 Ionawr 2019
Dyddiad yr Adolygiad Nesaf	Ionawr 2021

1. Diben

Diben y polisi hwn yw gosod safon ar gyfer creu cyfrineiriau cryf, amddiffyn y cyfrineiriau hynny, ac amlder newid.

2. Datganiad Polisi

Bydd y Brifysgol yn sicrhau bod ei hasedau gwybodaeth yn cael eu hamddiffyn yn briodol gan gyfrineiriau yn ôl yr angen a bod y cyfrineiriau hynny'n ddiogel yn dechnegol ac yn cael eu cadw'n ddiogel.

3. Cwmpas

3.1 Mae cwmpas y polisi hwn yn cynnwys pob defnyddiwr sydd â chyfrif, neu sy'n gyfrifol am un (neu unrhyw fath o fynediad y mae angen cyfrinair ar ei gyfer) ar unrhyw system yng nghyfleusterau Prifysgol Caerdydd, sydd â mynediad at rwydwaith Prifysgol Caerdydd, neu sy'n storio unrhyw wybodaeth am Brifysgol Caerdydd nad yw'n gyhoeddus. Mae hyn yn cynnwys pob system gyfrifiadurol, gan gynnwys cyfrineiriau, cynorthwywyr digidol personol (PDAs) a ffonau clyfar.

3.2 Nid yw defnyddio tystysgrifau digidol ar gyfer dilysu'n cael ei gynnwys yn y polisi hwn.

3.3 Lle na all systemau gefnogi'r cymhlethdod angenrheidiol ar gyfer y cyfrinair gweler adran 7 isod.

4. Cysylltiad â pholisïau sy'n bodoli'n barod

Mae’r polisi hwn yn rhan o’r Fframwaith Rheoli Diogelwch Gwybodaeth

Dylid darllen y polisi hwn ar y cyd â'r rheoliadau a pholisïau canlynol:

- Rheoliadau TG y Brifysgol
- Polisi Defnydd Derbyniol y Brifysgol
- Polisi Diogelwch TG y Brifysgol
- Canllawiau ar Ddefnydd Personol o Systemau TG Prifysgol Caerdydd

5. Amcanion y Polisi

5.1 Lle bo angen diogelu asedau gwybodaeth ar sail cyfrinachedd, gonestrwydd neu argaeledd bydd angen cyfrinair i gael mynediad at y systemau hynny sy'n cynnwys yr asedau.

5.2 Bydd cyfrineiriau a'r system sy'n eu gweithredu'n dilyn y safonau technegol a nodir isod.

- Dylid rhoi statws gwybodaeth gyfrinachol iawn i bob cyfrinair sy'n caniatáu mynediad at systemau Prifysgol Caerdydd.
- Unwaith y caiff hyn ei gyfleu i'r defnyddiwr gwreiddiol, ni ddylid rhannu cyfrineiriau na'u datgelu i rywun arall. Lle bo angen mynediad trydydd parti at gyfrif at ddibenion busnes dylid gwneud cais am gymorth drwy'r Ddesg Gwasanaeth TG a chynhelir proses ffurfiol ar gyfer newid y cyfrinair os bydd angen.
- Ni ddylid storio cyfrineiriau mewn modd nad yw'n ddiogel.
- Os rydych yn amau bod cyfrif neu gyfrinair wedi'i ddatgelu, rhowch wybod i Wasanaethau TG neu Weinyddwr y System am y digwyddiad ar unwaith.

6. Safonau Technegol

6.1 Gweinyddwyr System Gyfrifiadur

6.1.1 Dylai hyd y cyfrinair fod o leiaf 10 nod.

6.1.2 Dylai cyfrineiriau gynnwys cymysgedd o briflythrennau a llythrennau bach.

6.1.3 Dylai cyfrineiriau gynnwys o leiaf un rhif

6.1.4 Dylai cyfrineiriau ar lefel y system (sylfaenol, gweinyddwr) gynnwys o leiaf un nod arbennig.

6.1.5 Dylid sicrhau bod gosodiad er mwyn atal pobl rhag defnyddio cyfrineiriau cyffredin e.e. Password01.

6.1.6 Ni ddylid rhannu cyfrifon ar lefel y system (sylfaenol, gweinyddwr). Bydd gan bob gweinyddwr enw defnyddiwr a chyfrinair unigryw.

6.1.7 Dylid cadw hanes cyfrineiriau er mwyn atal ailddefnyddio cyfrineiriau o fewn 12 mis.

6.1.8 Lle mae system yn darparu naill ai nodweddion cloi tresmaswyr allan neu osgoi torri mewn dylid galluogi un o'r nodweddion i gael ei ddefnyddio. Ar gyfer cloi tresmaswyr allan argymhellir i gyfrifon gael eu cloi ar ôl methu â mewngofnodi 3 gwaith yn olynol.

6.1.9 Ni ddylid storio cyfrineiriau ar ffurf blaen heb ei amgryptio. Os yw'n bosibl, dylid defnyddio cryptograffeg anghymesur. Mae'n rhaid diogelu ffeiliau neu gronfeydd data er mwyn atal mynediad neu gopïo heb ei awdurdodi.

6.1.10 Ar gyfer adfer ar ôl chwalfa gellir cadw un copi ysgrifenedig o gyfrineiriau system mewn lleoliad diogel, er enghraifft gellir defnyddio sêff adrannol/ysgol neu gell cyfrinair megis KeePass (http://keepass.info/) .

6.1.11 Mae'n rhaid rheoli unrhyw achos o ddatgelu cyfrinair, yn sgil rhyng-gipio er enghraifft, yn ystod y broses o ddosbarthu cyfrineiriau i ddefnyddwyr. Cyfeiriwch at Ganllawiau Gwasanaethau TG ar Ddosbarthu Cyfrineiriau Cychwynnol i Ddefnyddwyr.

6.1.12 Mae'n rhaid bod cyfarwyddiadau ar sut i ailosod cyfrineiriau ar gael i ddefnyddwyr drwy weinyddwyr y system.

6.1.13 Lle y defnyddir SNMP, mae'n rhaid diffinio llinynnau'r gymuned fel rhywbeth arall oni bai am y gosodiadau arferol o "cyhoeddus", "preifat" a "system" ac mae'n rhaid iddynt fod yn wahanol i'r cyfrineiriau a ddefnyddir i fewngofnodi'n rhyngweithiol. Mae'n rhaid defnyddio botwm hash os yw ar gael (e.e. SNMPv2)

6.1.14 Ni argymhellir defnyddio cyfrineiriau sydd wedi'u mewnosod mewn sgriptiau rhaglenni na ffeiliau ffurfweddu. Lle nad oes dull amgen, mae'n rhad rheoli mynediad at sgript neu'r ffeiliau ffurfweddu er mwyn atal rhywun rhag datgelu cyfrineiriau heb awdurdod. Dylid monitro neu gofnodi mynediadau er mwyn canfod mynediadau heb awdurdod.

6.1.15 Mae'n rhaid bod gan gyfrifon defnyddwyr sydd wedi cael caniatâd i gael breintiau lefel y system drwy aelodaeth grŵp neu raglenni megis "sudo" gyfrinair sy'n wahanol o bob cyfrif arall sydd gan y defnyddiwr hwnnw.

6.2 Safonau Datblygu Rhaglenni

6.2.1 Mae'n rhaid i ddatblygwyr rhaglenni sicrhau bod eu rhaglenni'n cynnwys y rhagofalon diogelwch canlynol.

Rhaglenni:

a) Dylent gefnogi'r gwaith o ddilysu defnyddwyr unigol, nid grwpiau.

b) Ni ddylent storio cyfrineiriau mewn testun clir nac mewn ffordd y gellir ei wrthdroi'n hawdd.

c) Dylent ddarparu ffordd o reoli rolau, fel y gall un defnyddiwr gymryd dros swyddogaethau unigolyn arall heb orfod gwybod cyfrinair yr unigolyn hwnnw.

d) Dylent gefnogi RADIUS a/neu X.509 gyda system adfer diogelwch LDAP lle bynnag y bo hynny'n bosibl.

7. Trefniadau Pontio

7.1 Bydd systemau nad ydynt yn gallu bodloni'r meini prawf, yn dilyn asesiad risg priodol o'r wybodaeth a ddiogelir gan y cyfrinair, eu rhannu i mewn i 3 chategori.

7.1.1 Maent yn cynrychioli risg isel i'r Brifysgol hyd yn oed os yw'r cyfrinair wedi'i ddatgelu ac felly wedi'u heithrio o'r polisi cyfrinair (e.e. y cyfrinair i fewngofnodi i ficrosgop mewn labordy)

7.1.2 Maent yn risg canolig ac felly wedi'u heithrio am gyfnod penodol neu tan i'r rhyddhad mawr nesaf o gyfrineiriau ddigwydd yn seiliedig ar y rhyddhad hwnnw'n ychwanegu cymorth ar gyfer gofynion y cyfrinair uchod,

7.1.3 Maent yn cynrychioli risg uchel (e.e. cynnwys data cyfrinachol) a chânt eu heithrio am gyfnod (a bennir gan lefel y risg) tra bod darpariaeth arall yn cael ei defnyddio neu tan y gellir cyflwyno mesur gweithdrefnol i ychwanegu haen ychwanegol o ddiogelwch, gan liniaru'r risg – e.e. dim ond o ystafell a gaiff ei diogelu gan fynediad drwy system sganio cerdyn. y gellir cael mynediad at y system.

8. Cyfrifoldebau

8.1 Mae **pob defnyddiwr**

- yn gyfrifol am ddiogelwch eu cyfrineiriau eu hunain ac am roi gwybod am unrhyw achos posibl o ddatgelu cyfrinair eu hunain neu gyfrineiriau defnyddwyr eraill.

8.2 Mae'n rhaid i

- weinyddwyr system sicrhau bod y systemau y maent yn gyfrifol amdanynt, yn rhoi'r polisi cyfrinair hwn ar waith.

8.3 Prynwyr Systemau

8.3.1 Mae'n rhaid ystyried y polisi hwn wrth nodi a dewis neu ddylunio systemau cyfrifiadur a meddalwedd newydd.

9. Cydymffurfio

9.1 Gellir ymdrin ag achosion o dorri Polisi Cyfrinair Systemau TG fel mater disgyblu dan bolisïau disgyblu staff y Brifysgol neu'r Côd Disgyblu Myfyrwyr fel y bo'n briodol.