



POLISI DIOGELWCH GWYBODAETH

Dyddiad	Pwrpas Cyhoeddi/Disgrifiad o'r Newid	Cwblhau AEC	
Mehefin 2011 29ain Mawrth 2012	Cyhoeddiad Cyntaf		
	Trydydd cyhoeddiad		
8fed Mehefin 2015 28ain Ionawr 2019	Pedwerydd Cyhoeddiad Pumed CIPP D ^o ðL 9ia WT D .ó!	28ain Gorffennaf, 2015	
	Uwch Swyddog Cyfrifol	Cymeradwywyd gan	Dyddiad
Pennaeth Llywodraethu a Chydymffurfio	Ysgrifennydd y Brifysgol	Grŵp Tasg Cydymffurfio	28ain Ionawr, 2019

Polisi Diogelwch Gwybodaeth

1. Rhagarweiniad

1.1 Polisi Prifysgol Bangor yw y bydd

- [a] Yr wybodaeth a reolir ganddi (ar ffurf papur ac yn electronig) yn cael ei diogelu'n briodol er mwyn:
 - (i) sicrhau cydymffurfir â ddefwriaeth ac arweiniad perthnasol; a,
 - (ii) sicrhau bod y wybodaeth ar gael dim ond i'r rhai sydd ag angen dilys i fynd at y wybodaeth, a diogelu rhag mynediad heb awdurdod; a,
 - (iii) sicrhau bod cyfrinachedd yn cael ei ail-gynnwedd gille delir data trydydd parti neu ddata personol; a
 - (iv) sicrhau parhad busnes a gwarchod asedau;
 - (v) atal methiannau o ran cywirdeb, neu ymyriadau ag argaeledd yr wybodaeth honno.
- [b] Hyfforddir staff am bolisiau ac arferion diogelwch gwybodaeth
- [c] Mae cyngor arbenigol ar ddiogelwch gwybodaeth ar gael drwy'r brifysgol.
- [d] Mae systemau, technoleg a chymwysiadau'r brifysgol a ddefnyddir i gadw neu brosesu data personol, sensitif neu gyfrinachol yn ddiogel, yn ddilys a chedwir copïau wrth gefn.
- [e] Caiff unrhyw achosion o dorri rheolau diogelwch gwybodaeth, neu bu ond y dim iddynt gael eu torri, eu cofnodi i sicrhau bod camau priodol a mesurau ataliol yn cael eu gweithredu.

1.2 Mae'r Polisi Diogelwch Gwybodaeth hwn yn darparu cyfeiriad rheoli a chefnogaeth ar gyfer diogelwch gwybodaeth ar draws y Brifysgol. Bydd polisiau atodol penodol a chyfarwyddyd yn cael eu hystyried fel rhan o'r Polisi hwn. Drwy'r polisiau, y gweithdrefnau a'r strwythurau hyn, bydd y Brifysgol yn hwyluso llinn gwybodaeth yn ddiogel a hwn y Brifysgol ac ym mhob gohebiaeth allanol.

1.3 Cymeradwywyd y Polisi hwn gan y Grŵp Tasg Cydymffurfir i gadarnhau gan y Pwyllgor Gweithredu ac y mae'n rhan o bolisiau a gweithdrefnau Prifysgol Bangor. Y mae'n berthnasol i'r holl staff, myfyrwyr a thrydydd partion eraill perthnasol a bydd yn cael ei gyfleu iddynt.

1.4 Bob tro y torrir y Polisi hwn, bydd y bodamweiniol neu'n fwriadol, yn wirioneddol neu a amheuir, byddant yn cael eu hadrodd a'u hymchwilio'n unol ag Adran 8 y Polisi hwn.

2.

2.2 Mae gwybodaeth yn bodoli o fewn y Brifysgol ar sawl ffurf. Er enghraifft, gallon ni gwyb

- wedi'i hargraffu neu ei hysgrifennu ar bapur,
- wedi'i storio'n electronig,
- wedi'i throsglwyddo drwy'r post neu gan ddefnyddio dulliau electronig,
- wedi'i darlledu,
- ar lafar

3.

Diogelu Data

ffonau clyfar a thabledi gael eu diogelu gan rif PIN². Ni ddylid defnyddio dyfeisiau heb eu hamgryptio i gadw data'r brifysgol.

[iv] Mae modd gamerau fideo / recordyddion clywedol data yn ogystal, ac mae angen i wybodaeth gael ei ddiogelu yn ffisegol a drwy ei amgryptio (lle mae hyn yn bosib). Ni ddylid gadael data fideo neu ddata clywedol personol ar ddyfais heb ei amgryptio. Gweler Atodiad 1 am fwy o wybodaeth.

[iv] Nid yw'n bosibl, o fewn Office365, i aelodau staff anfon eu cyfrif e-bost cyfan ymlaen oddi ar y safle i westeibost drydydd parti. Os bydd aelodau staff yn dewis anfon ymlaen un neges, dylid gwneud hyn gan rhyngwladol i ofynion y polisi hwn a'r *Rheoliadau Defnydd Derbyniol*

[f] AdroddiañÀ. μ (Åg Û Ö ! a!q}{R" Þ q!}(Wc ð 8 q!p p] j r\$,uu\$ \)7\ flàw! j /C2_0

6.2 Bydd Deoniaid Colegau / Pnaethiaid Ysgol / y Carwyddwyr Gwasanaeth Proffesiynol (drwy swyddog priodol) yn atebol am sicrhau y cynhelir as

ATODIAD 1

Canllawiau Diogelwch Gwybodaeth

1. CadwGwybodaeth Personol yn Ddiogel

Rhaid i bob data personol gael ei gadw mewn amgylchedd diogel gyda mynediad yn cael ei reoli - bydd y

gwybod'. Cyn anfon atodiadau ymlaen o gwbl, dylech wirio nad yw'r wybodaeth ar gael iddynt drwy ryw ffordd ddiogel arall.

- [c] Defnyddio Adnoddau TG yn ddiogel i ffwrdd o'r Brifysgol
- [i] Wrth ddefnyddio eich PC neu MAC ac yn gweithio i ffwrdd o'r Brifysgol, dylech fod yn ymwybodol y gellid storio gwybodaeth ar y ddyfais honno mewn dwy ffordd allweddol:
- eich bod yn penderfynu storio ffeil ar y ddyfais neu;
 - drwy broses megis darllen atodiadau a ddaeth i'w gwybodaeth ei gadael ar y ddyfais yn anfwriadol heb i chi wybod.
- [ii] Y dull diogel weithio i ffwrdd o'r Brifysgol gan roi sylw priodol i Ddiogelwch gwybodaeth (e.e. ar un o liniaduron y Brifysgol neu ddiogelwch cyfrifiaduron heb fod yn eiddo i'r Brifysgol) yw drwy ddefnyddio gwasanaeth

- Dylech sicrhau bod eich dyfais wedi'i amgryptio (yn cynnwys unrhyw gardiau cof a all fod yn y ddyfais). Gofynnwch am gyngor y Gwasanaethau TG os oes angen.
- Sefydlu cyfrinair diogel neu rif PIN ar eich dyfais symudol. Pan na ddefnyddir y ddyfais am gyfnod amser, bydd yn cloi a bydd angen y cod diogelwch i'w defnyddio eto, sy'n ychwanegu gwarchodaeth pe digwydd i'r ddyfais gael ei cholli neu ei dwyn.
- Gwneud copïau wrth gefn o unrhyw ddata sydd ar eich dyfeisiau, megis dogfennau, delweddau ayb. Os byddwch yn gysoni eich bost, calendr a'ch cysylltiadau â'ch cyfrif Prifysgol, nid oes angen i chi wneud copïau wrth gefn o'r data hwn gan y caiff ei storio'n ganolog yn y Brifysgol a dim ond golwg ar y data hwn a geir ar eich dyfais. Fodd bynnag, os defnyddiwch ddelweddau neu ddata ychwanegol ar wahân i'ch cyfrif Prifysgol, dylech gopïo'r ffeiliau hyn yn rheolaidd i'ch PC, yn ddelfrydol, ffolder ar eich gyriant One Drive, i sicrhau bod gennych gopïau wrth gefn pe digwydd i'ch dyfais fethu neu fynd ar goll.

- Os nad oes gennych fynediad at ddyfais wedi'i hamgryptio ar gyfer eich recordiadau yna dylech ystyried a oes gen cofnodi'r wybodaeth. A oes dull arall, efallai gyda llai o risg, i gadw neu ddiogelu'r wybodaeth?
- Os ydych yn gorfod defnyddio dyfais heb ei hamgryptio, ar ôl cysidro pob opsiwn, yna bydd raid i chi gymryd camau ar unwaith i amgryptio'r data a ddelir. Ar ôl cwblhau'r sesiwn recordio dylid trosglwyddo'r cynnwys o'r cerdyn cof a ddefnyddiwyd i ddyfais wedi ei hamgryptio (gliniadur fel rheol). Yna dylid dileu'r ffeiliau o'r cerdyn cof. Yn yr un modd â chofion bach USB, pan gaiff ffeil

g)

tudalennau gwe a ddiogelwyd (mae cyfeiriad y rhain yn dechrau <https://> - y llythyren 's' yn nodi diogel).

- i) Bydd llawer o ffurflenni gwe yn gofyn a ydych yn dymuno arbed cyfrinair a ddarparwyd gennych. Ym mhob achos defnyddiwch yr opsiwn - "byth ar gyfer y wefan hon". Bydd hyn yn cynorthwyo i atal unrhyw fynediad heb awdurdod at unrhyw dudalenn

ATODIAD 2

FFURFLEN COFNODI DIGWYDDIAD DIOGELWCH GWYBODAETH

Eich Manylion

1. ENW .
2. ADRAN .
3. E-BOST .
4. RHIF FFÔN .

Manylion y Digwyddiad

1. Dyddiad y digwyddiad
2. Dyddiad yr adroddwyd ar y digwyddiad
3. Darparwch grynodeb byr o'r tor-diogelwch neu golled data. (nodwch y math o wybodaeth, megis data masnach neu bersonol, cofnodion meddygol, manylion ariannol, myfyrwyr neu staff):-
4. Rhowch wybod am unrhyw gamau dilynol neu gamau eraill a gymerwyd (os o gwbl).
5. Unrhyw wybodaeth arall y teimlwch sy'n berthnasol

Dychweler drwy e-bost at: Lynette Hunter, Swyddfa Llywodraethu a Chydymffurfio: info-compliance@bangor.ac.uk