# Polisi Diogelu Gwybodaeth

| | |
|---|---|
| Rhif y Fersiwn: | 2 |
| Statws y Ddogfen: | Cymeradwywyd |
| Dyddiad Cymeradwyo: | 19 Ebrill 18 |
| Cymeradwywyd Gan: | Grŵp Goruchwylio Rheoli Data a Gwybodaeth |
| Dyddiad Dod i Rym: | 19 Ebrill 18 |
| Dyddiad yr Adolygiad Nesaf: | Mawrth 2020 |

## 1 DIBEN A CHWMPAS

1.1 Diben y polisi hwn yw gosod nodau ac amcanion y Brifysgol ar gyfer rheoli diogelwch gwybodaeth ledled y Brifysgol. Diffiniad Diogelwch Gwybodaeth yw diogelu cyfrinachedd, uniondeb ac argaeledd gwybodaeth. Ceir diffiniadau pellach o'r holl dermau allweddol yn adran 5.

1.2 Mae cwmpas y Polisi Diogelu Gwybodaeth yn cynnwys storio, mynediad, trosglwyddo a dinistrio gwybodaeth yn ystod busnes Prifysgol Caerdydd. Felly mae'n berthnasol i ymddygiad staff, myfyrwyr ac eraill sydd â mynediad at y wybodaeth honno (lle bynnag mae'r wybodaeth neu maent hwy wedi'u lleoli) yn ogystal â'r cymwysiadau, systemau, cyfarpar ac adeiladau sy'n creu, prosesu, trosglwyddo, cynnal neu storio gwybodaeth, boed yn fewnol, wedi'i pherchen yn bersonol neu wedi'i darparu gan gyflenwyr allanol.

## 2 PERTHYNAS Â PHOLISÏAU SYDD EISOES YN BODOLI

Mae'r polisi hwn yn darparu'r dull o weithredu cyffredinol i reoli diogelwch gwybodaeth ym Mhrifysgol Caerdydd a dyma ddogfen bolisi meistr y fframwaith diogelwch gwybodaeth. Bydd yr holl bolisïau cysylltiedig yn gyson gyda'r polisi hwn.

## 3 DATGANIAD POLISI

Mae Prifysgol Caerdydd wedi ymrwymo i gadw cyfrinachedd, uniondeb ac argaeledd ei holl asedau gwybodaeth allweddol er mwyn cynnal ei mantais gystadleuol, cydymffurfiaeth gyfreithiol a chytundebol a'i henw da. Bydd y fframwaith diogelwch gwybodaeth (sy'n cynnwys y polisi hwn, polisïau cefnogol, prosesau ac offer a'r strwythurau rheoli a phenderfynu angenrheidiol) yn fecanwaith galluogi rhannu gwybodaeth ac i leihau'r risg sy'n gysylltiedig â gwybodaeth i lefelau derbyniol.

## 4 NODAU AC AMCANION DIOGELWCH GWYBODAETH

4.1 Bydd y fframwaith diogelwch gwybodaeth yn darparu amgylchedd cydymffurfio a *galluogi* sy'n cydbwyso diogelwch gwybodaeth gyda hygyrchedd priodol ac yn darparu'r lefel orau posibl o reoli risg i gefnogi cyflawniad nodau strategol y Brifysgol.

4.2 Mae diogelwch gwybodaeth wedi'i gynnwys mewn gweithgaredd ehangach rheoli data a gwybodaeth. Mae'r Brifysgol yn trefnu rheolaeth ei asedau gwybodaeth drwy ddefnyddio categorïau canlynol:

- Meysydd Data;
- Systemau TG;
- Dyfeisiau defnyddiwr terfynol;
- Pobl.

O dan y Fframwaith Llywodraethu Data a Gwybodaeth, mae gan bob un o'r uchod berchennog cyfrifol adnabyddadwy ac mae mesurau rheoli diogelwch gwybodaeth yn cael eu gweithredu ar draws y pedwar maes.

4.3 Bydd y Brifysgol yn gwarchod diogelwch ei asedau gwybodaeth er mwyn:

- cynnal uniondeb ac ansawdd gwybodaeth, fel ei bod yn gywir, yn gyfredol ac yn 'addas i'r diben';
- sicrhau bod gwybodaeth ar gael i'r rhai sydd ei hangen a sicrhau nad oes tarfu ar fusnes y Brifysgol;
- sicrhau ni thorrir ar gyfrinachedd, fel y ceisir gwybodaeth gan y rhai a awdurdodwyd i wneud hynny yn unig;

felly'n sicrhau bod y Brifysgol yn bodloni ei rhwymedigaethau cyfreithiol a rheoliadol mewn perthynas â thrin gwybodaeth, y cynhelir busnes yn effeithlon, y diogelir eiddo deallusol a bod enw da'r Brifysgol yn cael ei ddiogelu.

4.4 <u>Amcanion Diogelwch Gwybodaeth</u>

4.4.1 Bydd y Brifysgol yn rheoli'r risgiau y mae'n eu hwynebu mewn perthynas â diogelwch gwybodaeth, yn cadw ei amlygiad i awydd risg y Brifysgol. Bydd y strwythur llywodraethu yn cynnwys dyrannu perchnogaeth risgiau diogelwch gwybodaeth ac asedau gwybodaeth i ddarparu atebolrwydd, a sefydlu polisi asesu risg a phrosesau.

4.4.2 Bydd y dull asesu risg yn darparu dull cyson a systematig o ymdrin ag amcangyfrif maint y risgiau a'r broses o gymharu'r risgiau a amcangyfrifir yn erbyn meini prawf derbyn risg i benderfynu arwyddocâd y risgiau ac unrhyw newidiadau i risg dros amser.

4.4.3 Bydd y fframwaith hefyd yn creu cysondeb o ran dull o weithredu ac eglurder drwy sicrhau bod rolau a chyfrifoldebau diogelwch gwybodaeth yn cael eu diffinio a'u mynegi'n glir drwy ddogfennau polisi, contractau a swydd ddisgrifiadau a bod dealltwriaeth yn cael ei hatgyfnerthu drwy hyfforddiant wedi'i fonitro, gweithdrefnau wedi'u dogfennu, prawf ac adolygiadau datblygu perfformiad blynyddol, fel bod pob unigolyn yn deall eu rôl a'u cyfrifoldeb o ran diogelwch gwybodaeth.

4.4.4 Bydd y Brifysgol yn sicrhau bod gwybodaeth diogelwch gwybodaeth yn rheolaethau diogelwch gwybodaeth briodol a rennir a chymhwyso yn y modd mwyaf effeithlon, effeithiol a darbodus gan gynnal trosolwg lefel uchel drwy'r corff sy'n cydlynu; gan ymgorffori ystyriaethau diogelwch gwybodaeth i gynllunio, pontio, a darparu gwasanaethau; a thrwy wneud arfau angenrheidiol a'r Cyngor ar ddiogelwch gwybodaeth sydd ar gael ledled y brifysgol, fel y gall pob unigolyn gael gafael ar y Cyngor perthnasol, polisi, gweithdrefn, hyfforddiant neu offer mewn modd amserol.

4.4.5 Er mwyn lleihau nifer a difrifoldeb y digwyddiadau diogelwch gwybodaeth, a sicrhau y cymerir camau priodol o ran adrodd i awdurdodau allanol perthnasol, bydd system cofnodi, adrodd a rheoli digwyddiadau diogelwch gwybodaeth yn cael ei gweithredu a'i monitro, gyda chanlyniadau'n hysbysu asesiadau risg yn y dyfodol.

4.4.6 Bydd diwylliant cefnogol ar gyfer diogelwch gwybodaeth yn cael ei greu o fewn y Brifysgol drwy gyfeiriad rheoli clir a rheolaeth unigol sy'n dangos ymrwymiad i'r fframwaith diogelwch gwybodaeth, gan gynnwys cydnabyddiaeth ac aseiniad eglur o gyfrifoldebau diogelwch gwybodaeth, ymrwymiad i ymgymryd â hyfforddiant ac adrodd am ddigwyddiadau diogelwch.

4.4.7 Bydd y Brifysgol yn sicrhau bod ei fframwaith diogelwch gwybodaeth yn addas i'r diben drwy ddefnyddio Gofynion Diogelwch Gwybodaeth ISO/IEC 27001:2013, drwy gynnal archwiliadau rheolaidd a thrwy broses o welliant parhaus, yn meincnodi ei hun mewn perthynas â diogelwch gwybodaeth yn erbyn sefydliadau cymharol lle y bo'n bosibl.

## 5 CYFRIFOLDEBAU

### 5.1 Y Cyngor

Mae gan y Cyngor atebolrwydd yn y pen draw ar gyfer gweithgareddau diogelwch gwybodaeth o fewn y Brifysgol. Yn fwy penodol, mae'n amddiffyn enw da sefydliadau drwy gael sicrwydd bod rheoliadau, polisïau a gweithdrefnau clir sy'n glynu at ofynion deddfwriaethol a rheoliadol yn eu lle, yn foesegol eu natur, ac yn cael eu dilyn. Mae angen i'r Cyngor fod yn sicr bod systemau effeithiol o reoli a rheoli risg a bod prosesau a strwythurau llywodraethu yn addas i'r diben gan eu cyfeirio yn erbyn safonau ymarfer da cydnabyddedig.

### 5.2 Bwrdd Gweithredol y Brifysgol

Mae Bwrdd Gweithredol y Brifysgol yn gyfrifol drwy'r Is-Ganghellor i'r Cyngor ar gyfer:

- arwain a meithrin diwylliant sy'n gwerthfawrogi, yn diogelu ac yn defnyddio gwybodaeth ar gyfer llwyddiant y Brifysgol a budd ei aelodau;

- diffinio awydd risg diogelwch gwybodaeth y Brifysgol yn y cyd-destun cyfreithiol, gwleidyddol, cymdeithasol-economaidd, yr amgylchedd technolegol a safonau allanol;
- sicrhau bod fframwaith diogelwch gwybodaeth sy'n addas i'r diben gydag adnoddau digonol ar waith, gan gynnwys y polisi hwn fel dogfen gyfeirio lefel uchaf.

5.3 Uwch-berchennog Risg Gwybodaeth

Bydd yr Is-Ganghellor yn dynodi Uwch-berchennog Risg Gwybodaeth (SIRO) ar gyfer amcanion diogelwch gwybodaeth cyffredinol y Brifysgol. Bydd y SIRO hefyd yn aelod o Fwrdd Gweithredol y Brifysgol. Cyfrifoldebau allweddol y SIRO bydd:

- sicrhau bod y polisi hwn ac amcanion diogelwch gwybodaeth yn gydnaws â chyfeiriad strategol y Brifysgol;
- sicrhau y nodir asedau data a gwybodaeth; bod rolau llywodraethu gwybodaeth a data lefel uchaf yn cael eu dyrannu a bod deiliaid y sydd yn cael eu briffio'n briodol ar eu rolau diogelwch gwybodaeth ac yn cyflawni eu swyddogaethau gyda diwydrwydd dyledus;
- yn berchen ar y risgiau sy'n gysylltiedig ag amcanion diogelwch gwybodaeth a sicrhau bod perchnogion camau rheoli yn cael eu nodi;
- sicrhau bod gweithdrefnau eithriad ar waith i awdurdodi ar lefel briodol derbyn neu liniaru risgiau diogelwch gwybodaeth sylweddol sy'n gwyro o'r safonau y cytunwyd arnynt;
- penderfynu pryd a chan bwy yr adroddir ar achosion o dorri diogelwch gwybodaeth i awdurdodau allanol perthnasol;
- sicrhau bod cyfeiriad clir a chymorth rheoli gweladwy ar gyfer mentrau diogelwch a hyrwyddo gwelliant parhaus;
- sicrhau bod yr Is-Ganghellor a'r Cyngor yn cael eu briffio'n ddigonol ar faterion rheoli risg.

5.4 Grŵp Goruchwylio Rheoli Data a Gwybodaeth

Y Grŵp Goruchwylio Rheoli Data a Gwybodaeth sy'n gyfrifol am roi cyfeiriad strategol a ffocws i weithgareddau rheoli data a gwybodaeth ar draws y Brifysgol. Mae'r cwmpas yn cynnwys ansawdd data a diogelwch gwybodaeth.

Mae'r Grŵp Goruchwylio Rheoli Data a Gwybodaeth yn rhoi sicrwydd i Fwrdd Gweithredol y Brifysgol drwy'r Uwch-berchennog Risg Gwybodaeth/Prif Swyddog Gweithredu a fydd yn cadeirio'r Grŵp Goruchwylio Rheoli Data a Gwybodaeth. Nodir y cylch gorchwyl yn Atodiad A.

5.5 Rolau Llywodraethu Data a Gwybodaeth

Bydd rolau Cefnogol Llywodraethu Data a Gwybodaeth yn cael eu sefydlu gan yr Uwch-berchennog Risg Gwybodaeth (Atodiad B)

5.6 Penaethiaid Ysgolion/Adrannau/Colegau

- yn gyfrifol am:

– wneud yn siŵr bod staff yn ymwybodol bod angen cadw at y polisi hwn a pholisïau cysylltiedig am ddiogelwch gwybodaeth;
– rhoi gwybod am achosion o beidio â chydymffurfio drwy'r sianeli cymeradwy a ddiffinnir.

5.7 Pob defnyddiwr

Bydd holl ddefnyddwyr unigol systemau gwybodaeth y Brifysgol a'r rheiny sy'n trin neu'n cael mynediad at wybodaeth y Brifysgol y tu allan i'r systemau hynny yn gyfrifol am:

- gydymffurfio â'r holl bolisïau, ymarferion a gweithdrefnau diogelwch gwybodaeth perthnasol, gan gynnwys unrhyw atebolrwydd allanol;
- sicrhau eu bod yn gwneud cais, lle y bo angen, ac yn derbyn hyfforddiant ymwybyddiaeth o ddiogelwch gwybodaeth digonol a pherthnasol i'w galluogi i gyflawni eu swyddogaethau; ac
- adrodd ar ddigwyddiadau diogelwch gwybodaeth drwy'r sianeli cymeradwy a ddiffiniwyd.

## 6 ACHOSION O DORRI POLISÏAU

Gellir ymdrin ag achosion o Dorri'r Polisi Diogelu Gwybodaeth fel mater disgyblu dan bolisïau disgyblu staff y Brifysgol neu'r Cod Disgyblu Myfyrwyr fel y bo'n briodol.

## 7 DIFFINIADAU

| | |
|---|---|
| **Argaeledd** | Cael mynediad priodol at Asedau Gwybodaeth yn ôl yr angen, yn rhan o waith y Brifysgol. |
| **Cyfrinachedd** | Cyfyngu gwybodaeth i'r unigolion hynny sydd ag awdurdod i'w derbyn neu ei gweld. |
| **Gwybodaeth** | Data sydd ag ystyr neu ddata y gellir ei ddehongli. Gellir ei gadw ar ffurf cofnod electronig neu mewn fformat nad yw'n electronig megis papur, microfiche, llun |
| **Ased Gwybodaeth** | Gwybodaeth sydd â gwerth i'r Brifysgol. Asedau Gwybodaeth Allweddol yw'r mathau pwysicaf o wybodaeth sy'n ofynnol er mwyn cyflawni nodau strategol y Brifysgol |
| **Gonestrwydd** | Pa mor gyflawn a gwarchodedig yw'r wybodaeth, yn ei ffurf wreiddiol a bwriadedig, oni bai bod pobl neu brosesau awdurdodedig wedi'i newid neu ei dileu. |
| **Ansawdd** | Y cyflwr o gyflawnder, dilysrwydd, cysondeb, amseroldeb a chywirdeb sy'n gwneud data yn briodol ar gyfer defnydd gweithredol a strategol. |

**ATODIAD A**

**Cylch Gorchwyl y Grŵp Goruchwylio Rheoli Data a Gwybodaeth**

Mae'r Grŵp Goruchwylio Rheoli Data a Gwybodaeth yn gyfrifol am roi cyfeiriad strategol a ffocws i weithgareddau rheoli data a gwybodaeth ar draws y Brifysgol. Mae'r cwmpas yn cynnwys ansawdd data a diogelwch gwybodaeth.

Mae'r Grŵp Goruchwylio Rheoli Data a Gwybodaeth yn rhoi sicrwydd i Fwrdd Gweithredol y Brifysgol drwy'r Uwch-berchennog Risg Gwybodaeth/Prif Swyddog Gweithredu a fydd yn cadeirio'r Grŵp Goruchwylio Rheoli Data a Gwybodaeth.

1. adolygu a chymeradwyo portffolio'r Brifysgol o ddata a pholisïau rheoli gwybodaeth i sicrhau ei bod yn parhau i gyd-fynd ag amcanion strategol y Brifysgol
2. monitro ac adolygu amlygiad y Brifysgol i risg ym meysydd llywodraethu data a gwybodaeth;
3. darparu ffocws strategol ar gyfer cymhwysiad data a gwybodaeth mesurau rheoli diogelwch ac ansawdd ar draws gwybodaeth ac asedau, yn seiliedig ar ddull asesu risg o weithredu;
4. sicrhau bod safonau yn cael eu gosod a'u hadolygu o bryd i'w gilydd
5. ystyried ceisiadau am eithriadau a rhoi awdurdod lle y bo'n briodol
6. cyfathrebu a hyrwyddo gwerth asedau data a gwybodaeth
7. sicrhau bod hyfforddiant digonol ar waith i gefnogi amcanion rheoli gwybodaeth a data'r Brifysgol
8. monitro ac adolygu ymateb y Brifysgol i ddigwyddiadau diogelwch gwybodaeth;
9. adolygu canfyddiadau archwilio llywodraethu data a gwybodaeth ac argymhellion.

**ATODIAD B: Rolau Cefnogol Llywodraethu Data a Gwybodaeth**

| RÔL | LEFEL | CYFRIFOLDEBAU |
|---|---|---|
| **Uwch-berchennog Risg Gwybodaeth** | **Aelod o'r Bwrdd Gweithredol** | Yn atebol am sicrhau bod y polisi diogelu gwybodaeth a rheoli data, ac amcanion cysylltiedig, yn cyd-fynd â chyfeiriad strategol y Brifysgol; yn berchen ar y risgiau sy'n gysylltiedig â'r amcanion cysylltiedig a sicrhau bod perchnogion gweithredu rheoli'n cael eu nodi, gan gynnwys nodi Asedau Gwybodaeth allweddol, Arweinwyr Data ac Uwch-berchnogion System; yn awdurdodi derbyn neu liniaru risgiau diogelwch gwybodaeth sylweddol sy'n gwyro o'r safonau y cytunwyd arnynt; yn penderfynu pryd a chan bwy yr adroddir ar achosion o dorri diogelwch gwybodaeth i awdurdodau allanol perthnasol; sicrhau bod cyfeiriad clir a gweladwy o ran cymorth rheoli ar gyfer rheoli data a mentrau diogelwch a hybu gwelliant parhaus; yn sicrhau bod yr Is-Ganghellor a'r Cyngor yn cael eu briffio'n ddigonol ar faterion rheoli risg.<br>Uwch-ddolen Gyswllt ar gyfer HESA. |
| **Arweinydd Data** | **Cyfarwyddwyr Gwasanaethau Proffesiynol** | Yn atebol am ansawdd y data o fewn eu maes; Yn sicrhau bod data o fewn y maes yn addas ar gyfer defnydd gweithredol a strategol; Yn pennu amodau pan gall data gael ei ddefnyddio (gan ystyried unrhyw rwymedigaethau cyfreithiol sy'n berthnasol i'r math hwnnw o ddata), er mwyn diogelu cyfrinachedd, uniondeb, argaeledd ac ansawdd; Yn cadarnhau dosbarthiadau endidau data o fewn y maes; Yn cadarnhau gofynion data ar gyfer dibenion busnes. |
| **Uwch-berchnogion System (Busnes)** | **Cyfarwyddwyr** | Yn cadarnhau dibenion busnes a chanlyniadau gofynnol systemau; Yn atebol ar gyfer mesurau rheoli penodol i system i sicrhau diogelwch ac ansawdd y data, gan gynnwys cydymffurfio â thelerau unrhyw drwydded 3ydd parti neu delerau cytundebol eraill sy'n gymwys i fynediad y Brifysgol at y system, neu ei defnydd a ganiateir ohoni; Yn enwebu Perchnogion System (Busnes) ar gyfer systemau pwrpasol; Yn cadarnhau gofynion cytundeb lefel gwasanaeth parthed argaeledd y system. |
| **Uwch-berchennog Systemau (Technegol)** | **Prif Swyddog Gwybodaeth** | Yn atebol am agweddau technegol ar systemau i sicrhau diogelwch a chywirdeb data; Yn enwebu Perchnogion System (Technegol) |

| | | |
|---|---|---|
| **Stiward Data Prifysgol** | **Cyfarwyddwr Cynllunio Strategol a Llywodraethu** | Yn ganolwr terfynol dros benderfyniadau sy'n effeithio ar berthnasau rhwng meysydd data a gwrthrychau; Yn ganolwr terfynol dros benderfyniadau sy'n effeithio ar drawsnewidiadau gwrthrychau data; Yn cydgysylltu adrodd ar ddata allanol yn strategol; Yn goruchwylio camau i weithredu fframweithiau rheoli data a diogelwch gwybodaeth (gan gynnwys rheoli digwyddiadau diogelwch gwybodaeth), gan sicrhau eu bod yn cael eu hadolygu o bryd i'w gilydd ac yn parhau i fod yn addas i'r diben. |
| **Perchennog System (Technegol)** | **Uwch Reolwr (TG) / Cyflenwr gwasanaeth** | Yn adeiladu a chynnal system i gwrdd â dyluniad y cytunwyd arno; Yn sefydlu a chynnal trosglwyddiadau data; Yn gweithredu mesurau rheoli dilysu a chaniatáu mynediad; Yn gweithredu mesurau rheoli gwrth-firws a maleiswedd; Yn gweithredu gallu wrth gefn ac adfer; Yn gweithredu mesurau rheoli priodoledd defnyddiwr technegol; Yn gweithredu gallu archwilio gallu ac yn cynhyrchu adroddiadau monitro fel sy'n ofynnol; Yn gweithredu cadw system a gofynion gwaredu; Yn gweithredu mesurau rheoli ansawdd data system; Yn darparu metrigau ar gyfer asesu risg; Yn datblygu gweithdrefnau ansawdd data technegol a diogelwch gwybodaeth. |
| **Perchennog System (Busnes)** | **Uwch-reolwyr** | Yn gyfrifol am fesurau rheoli polisi penodol i system er mwyn sicrhau diogelwch ac ansawdd y data; Yn diffinio anghenion data gofynnol ac allbynnau o gymwysiadau/systemau; Yn sicrhau cydbwysedd rhwng anghenion cyfrinachedd, uniondeb ac argaeledd y wybodaeth o dan eu rheolaeth er budd gorau'r Brifysgol ac yn unol â derbyn risg y cytunwyd arno; Yn cadarnhau grwpiau/rolau defnyddwyr system â chaniatâd cysylltiedig; Yn diffinio priodoleddau defnyddiwr ac amgylcheddau mynediad priodol; Yn diffinio gofynion wrth gefn ac adfer priodol; Yn dogfennu Manyleb Diogelwch Gwybodaeth ar gyfer pob system; Yn dogfennu Manyleb Diogelwch Gwybodaeth ar gyfer pob system; Yn diffinio gofynion system archwilio a monitro adroddiad; Mewn cysylltiad ag enwebeion Arweinwyr Data yn diffinio gofynion cadw a gwaredu ar gyfer cofnodion system; Yn asesu risgiau i ddiogelwch data o fewn systemau; Mewn cysylltiad ag enwebeion Arweinwyr Data, yn diffinio prosesau a gweithdrefnau ansawdd a diogelwch data sy'n benodol i'r system. |
| **Stiwardiaid Data** | **Uwch-reolwyr** | Yn gweithio gyda Pherchnogion System sicrhau bod ansawdd yr endidau data yn ddigonol i ateb y gofynion ar gyfer defnydd gweithredol a defnydd gwybodaeth busnes strategol; Yn diffinio ystyr endidau data; Yn cadarnhau ac adolygu dosbarthiadau endidau data; Yn asesu risgiau i ansawdd y data a chynghori Perchnogion System perthnasol; Yn penderfynu ar wiriadau ansawdd data gofynnol a mesurau rheoli a chynghori Perchnogion System; Yn newid rheoli pan fydd diffiniadau data yn newid; Yn diffinio gofynion o ran cadw ar gyfer endidau data |