**Polisi Rheoli Digwyddiad Diogelwch Gwybodaeth**

# Diben a Chwmpas

Diben y polisi hwn yw sicrhau dull cyson ac effeithiol o reoli Digwyddiadau Diogelwch Gwybodaeth, rhoi diffiniad o’r hyn yw Digwyddiad Diogelwch Gwybodaeth a sefydlu strwythur ar gyfer adrodd ynghylch digwyddiadau o'r fath a’u rheoli. Mae'r polisi hwn yn cefnogi'r brifysgol i ddangos ei chydymffurfiaeth â deddfwriaeth diogelu data, sy'n cynnwys yn bennaf Rheoliad Diogelu Data Cyffredinol y DU (GDPR y DU) a Deddf Diogelu Data 2018 (DPA 2018), o ran data unigolion, a'r rheoleiddiwr diogelu data a phreifatrwydd yn y DU (Comisiynydd Gwybodaeth).

Mae’r polisi hwn yn berthnasol i aelodau Prifysgol Caerdydd fel y’i diffinnir dan Ordinhad 2 – Aelodau’r Brifysgol ac unrhyw un arall sydd ynghlwm lle caiff data personol ei brosesu ar ran Prifysgol Caerdydd.

# Y Polisi

Bydd Prifysgol Caerdydd yn mynd i'r afael bob amser â digwyddiadau diogelwch gwybodaeth yn effeithlon ac yn effeithiol ac yn sicrhau eu bod yn cael eu rheoli yn unol â'r Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli

Bydd pob aelod o'r Brifysgol yn ymwybodol o'r weithdrefn ar gyfer rhoi gwybod am Ddigwyddiadau Diogelwch Gwybodaeth a'u cyfrifoldeb i roi gwybod am ddigwyddiadau o'r fath.

Bydd difrifoldeb y digwyddiad yn cael ei asesu a bydd ymateb y rheolwyr yn gymesur â'r bygythiad, ac fe elwir ar y Cynllun Digwyddiad Mawr lle bo'n briodol, er mwyn lleihau'r risgiau a'r effaith andwyol ar unrhyw bersonau perthnasol. Bydd staff perthnasol yn cael eu hyfforddi o ran casglu, cadw a chyflwyno tystiolaeth ddigidol, yn unol â rhwymedigaethau deddfwriaethol neu reoleiddiol.

Bydd risgiau newydd a nodir o ganlyniad i ddigwyddiad yn cael eu neilltuo i'r perchennog risg perthnasol a bydd risgiau derbyniol yn cael eu lliniaru'n brydlon yn unol â phrosesau rheoli risgiau'r brifysgol ac yn unol â'r Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli.

Caiff gwybodaeth allweddol ynghylch digwyddiadau Diogelwch Gwybodaeth difrifol, gan gynnwys effaith y digwyddiad (ariannol neu fel arall), ei chofnodi'n ffurfiol a chaiff y cofnodion eu dadansoddi er mwyn asesu effeithiolrwydd rheolaethau diogelwch gwybodaeth.

Bydd risgiau newydd a nodir o ganlyniad i ddigwyddiad yn cael eu neilltuo i'r perchennog risg perthnasol a bydd risgiau derbyniol yn cael eu lliniaru'n brydlon yn unol â phrosesau rheoli risgiau'r brifysgol ac yn unol â'r Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli.

Digwyddiad diogelwch gwybodaeth yw sefyllfa annymunol neu annisgwyl sy'n digwydd neu’n datblygu, sy’n dangos naill ai:

1. achos posibl o dorri polisi fframwaith diogelwch gwybodaeth neu
2. methiant o ran cadw at reolaethau diogelwch gwybodaeth, sydd â thebygolrwydd sylweddol o beryglu gweithrediadau busnes.

Mae'r diffiniad hwn yn berthnasol i weithredu neu ddiffyg gweithredu gan aelodau Prifysgol Caerdydd ac unrhyw un o'i his-gontractwyr sy'n prosesu gwybodaeth Gyfrinachol y brifysgol. Mae enghreifftiau o Ddigwyddiadau Diogelwch Gwybodaeth yn cynnwys y canlynol (ond nid yn gyfyngedig iddynt):

* Datgeliad damweiniol neu anawdurdodedig o wybodaeth Cyfrinachol C1 'Cyfrinachol Iawn' neu C2 'Cyfrinachol' gan gynnwys data personol (e.e. drwy ohebiaeth wedi'i hanfon i’r cyfeiriad anghywir, atodiad anghywir wrth gofnod neu ganiatâd mynediad anghywir at system/methiant hidlo system)
* Achos o golli neu ddwyn Gwybodaeth Gyfrinachol C1/C2 yn uniongyrchol (e.e. papurau yn cael eu dwyn o'ch car, post yn cael ei ddwyn cyn iddo gyrraedd, lawrlwytho heb ganiatâd)
* Achos o golli neu ddwyn cyfarpar a ddefnyddir i storio Gwybodaeth Gyfrinachol C1/C2 (e.e. gliniadur, ffôn clyfar, cofbin USB)
* Llygru neu addasu cofnodion hanfodol heb awdurdod (e.e. newid prif gofnodion)
* Peryglu system neu gyfarpar cyfrifiadurol (e.e. feirws, maleiswedd, ymosodiad atal gwasanaeth)
* Peryglu cyfrif defnyddiwr TG (e.e. ffugio, hacio, rhannu cyfrinair)
* Achos o dorri mewn i leoliad sydd â Gwybodaeth Gyfrinachol neu sydd â chyfarpar hanfodol ar gyfer prosesu data megis gweinyddion

Bydd digwyddiadau diogelwch gwybodaeth yn cael eu huwchgyfeirio yn unol â'r meini prawf rheoli risg yn y Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli, a bydd unigolion awdurdodedig yn rhoi gwybod amdanynt i'r awdurdodau allanol priodol lle bo'n berthnasol.

# Rolau a Chyfrifoldebau

Mae pob aelod o'r brifysgol yn gyfrifol am roi gwybod am Ddigwyddiadau Diogelwch Gwybodaeth gwirioneddol neu amheuaeth o hyn yn uniongyrchol i Ddesg y Gwasanaeth TG heb oedi gormodol yn unol â'r Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth a’u Rheoli. Ni chaniateir gweithdrefnau lleol sy'n gwrthdaro â hyn.

Bydd methu â rhoi gwybod am Ddigwyddiadau Diogelwch Gwybodaeth ac unrhyw achosion eraill sy'n torri'r polisi hwn yn cael ei ystyried yn fater disgyblu a rhoddir gwybod amdano i’r Uwch-berchennog Risg Gwybodaeth er mwyn iddynt fynd i'r afael â'r mater yn unol â’r weithdrefn disgyblu/ymddygiad perthnasol.

Bydd yn ofynnol i gontractwyr (gan gynnwys eu hasiantau a'u his-gontractwyr) sy'n gwneud gwaith ar systemau a gwasanaethau gwybodaeth y brifysgol nodi unrhyw wendidau diogelwch gwybodaeth sylweddol yn y systemau neu'r gwasanaethau hynny a rhoi gwybod amdanynt.

Caiff y cyfrifoldeb am ymateb i ddigwyddiadau diogelwch gwybodaeth ei nodi yn y Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli.

Uwch-berchennog y Risg Gwybodaeth sy’n gyfrifol am roi gwybod i awdurdodau allanol am Ddigwyddiadau Diogelwch Gwybodaeth difrifol oni bai bod y cyfrifoldeb wedi’i ddirprwyo fel arall yn y Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli.

Bydd Penaethiaid Ysgol/Cyfarwyddwr Gwasanaethau Proffesiynol yn gyfrifol am fonitro cydymffurfiaeth eu hadran â Pholisi Rheoli Digwyddiadau Diogelwch Gwybodaeth y Brifysgol.

# Polisïau a gweithdrefnau cysylltiedig

Mae’r polisi hwn yn rhan o’r Fframwaith Rheoli Diogelwch Gwybodaeth. Dylid ei ddarllen hefyd ar y cyd â’r**:**

* Weithdrefn Adrodd Ynghylch Digwyddiadau Diogelwch Gwybodaeth A’u Rheoli
* atodiad Adrodd Ynghylch Pryderon A’u Rheoli yn y Polisi Diogelu Oedolion a Phlant sy'n Agored i Niwed
* Polisi a Gweithdrefn Diogelu Data Talu â Cherdyn

**Tabl Rheoli’r Fersiwn**

|  |  |  |
| --- | --- | --- |
| Enw’r Ddogfen | Polisi Rheoli Digwyddiadau Diogelwch Gwybodaeth | |
| Noddwr Polisi Bwrdd Gweithredol y Brifysgol | Uwch-berchennog Risg Gwybodaeth – Ysgrifennydd y Brifysgol a’r Cwnsler Cyffredinol | |
| Perchennog y Polisi | Uwch Gynghorydd Cydymffurfio a Swyddog Diogelu Data, Swyddfa Ysgrifennydd y Brifysgol | |
| Awdur(on) y Polisi | Uwch Gynghorydd Cydymffurfio a Swyddog Diogelu Data, Swyddfa Ysgrifennydd y Brifysgol | |
| Rhif y Fersiwn | 1.1 | |
| Canlyniad yr Effaith ar Gydraddoldeb a Dyddiad Cyflwyno’r Ffurflen |  |  |
| Dyddiad Cymeradwyo | Mehefin 2023 | |
| Cymeradwywyd Gan | Uwch-berchennog Risg Gwybodaeth | |
| Dyddiad Gweithredu | Gorffennaf 2023 | |
| Dyddiad yr Adolygiad Diwethaf | Ebrill 2018 | |
| Dyddiad yr Adolygiad Nesaf | Gorffennaf 2024 | |
| At Ddefnydd y Swyddfa – Allweddeiriau ar gyfer y nodwedd chwilio |  | |