CYNGOR BWRDEISTREF SIROL RHONDDA CYNON TAF

GWEITHDREFN AR GYFER YMCHWILIO I DDIGWYDDIADAU AC ACHOSION YN YMWNEUD Â DIOGELWCH GWYBODAETH

Fersiwn: TERFYNOL v.1.5 wef 22.10.2025

Cynnwys

1.	Adolygiad Cychwynnol o Alwad Diogelwch	4
2.	Mynd i'r afael â Digwyddiad Diogelwch Gwybodaeth	5
3.	Mynd i'r afael ag Achos Seiberddiogelwch Gwybodaeth	5
4.	Mynd i'r afael ag Achos Diogelwch Gwybodaeth	6
5.	Achosion sy'n Ymwneud â Data Personol	7
6.	Camau Gweithredu ac Argymhellion a nodwyd yn ystod Ymchwiliad	8

Atodiad

I	Llif Gwaith Cyfeirio Cyflym: Ymchwilio i Achosion a Digwyddiadau Diogelwch Gwybodaeth	9

Cyflwyniad

Yn unol â Pholisi Diogelwch Gwybodaeth y Cyngor, rhaid cynnal dull ymdrin ag achosion a digwyddiadau sy'n ymwneud â diogelwch gwybodaeth cyson a chadarn ar draws y Cyngor. Rhaid trin ac ymchwilio i bob achos a digwyddiad yn briodol er mwyn sefydlu'r ffeithiau, nodi camau cywirol ac ataliol, a sicrhau bod data, systemau ac asedau'r Cyngor yn cael eu diogelu'n barhaus.

Mae'r weithdrefn yma'n nodi'r camau i'w dilyn wrth **ymchwilio** i unrhyw achos neu ddigwyddiad diogelwch gwybodaeth, ac mae'n berthnasol i bob gweithiwr, aelod etholedig, contractwr, cyflenwr trydydd parti, ac unrhyw un sydd â mynediad at ddata, systemau neu asedau'r Cyngor.

Dogfennau Perthnasol:

Dylid darllen y weithdrefn yma ar y cyd â gweithdrefnau'r Cyngor **Gweithdrefn ar gyfer Rhoi Gwybod am Ddigwyddiadau ac Achosion yn ymwneud â Diogelwch Gwybodaeth**, sy'n amlinellu sut y dylid rhoi gwybod am achosion a digwyddiadau. Mae'r ddwy ddogfen, ynghyd â'r Polisi Diogelwch Gwybodaeth, i'w gweld ar RCT Source neu Inform (*Gwasanaethau Cymorth > Rheoli Gwybodaeth > Polisïau)*.

Nodyn ar gyfer Aelodau Etholedig:

Dylai Aelodau Etholedig gyfeirio at y **Polisi Defnydd Derbyniol ar y Rhyngrwyd a Chyfleusterau E-bost a ThGCh yr Aelodau Etholedig** a Phorth yr Aelodau i gael mynediad at ddogfennaeth berthnasol a chanllawiau ar eu cyfrifoldebau penodol.

1. Adolygiad Cychwynnol o Alwad Diogelwch

Pan fydd galwad diogelwch gwybodaeth yn cael ei gwneud gan Ddesg Gwasanaeth TGCh, caiff ei hanfon at y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch am adolygiad cychwynnol, gan ddibynnu ar natur y mater.

Y cam cyntaf yw asesu natur y pryder diogelwch (e.e. a yw'n gysylltiedig â mater seiberddiogelwch, tor diogelwch data personol ac ati). Os mae data personol ynghlwm, mae'n bwysig penderfynu a yw tor diogelwch data personol wedi digwydd. Diffiniad tor diogelwch data personol yw pan gaiff gwybodaeth ei pheryglu ac mae'n arwain at ddinistrio, colli, addasu a/neu ddatgelu data personol heb awdurdod, neu fynediad anawdurdodedig at y data yna, a hynny drwy ddamwain neu'n fwriadol. Mae hyn yn cynnwys digwyddiadau damweiniol a bwriadol ac nid yw'n gyfyngedig i golli data personol.

Yn dilyn yr asesiad yma, bydd yr alwad yn cael ei dosbarthu fel naill ai **digwyddiad** neu **achos**:

- **Digwyddiadau**

  Fel arfer, mae digwyddiadau yn doriadau diogelwch posibl neu fewnol. Dyma enghreifftiau:
  - Gwall cyfathrebu mewnol (e.e. e-bost wedi'i anfon at yr adran neu'r swyddog anghywir)
  - Colli dyfais wedi'i hamgryptio sy'n cynnwys data personol (e.e. ffôn symudol, gliniadur, llechen)

- **Achosion**

  Mae achosion yn fwy difrifol ac wedi, neu'n debygol o, arwain at dor diogelwch a allai beryglu cyfrinachedd, uniondeb, neu argaeledd data, systemau neu asedau'r Cyngor. Dyma enghreifftiau:
  - Gwall cyfathrebu allanol (e.e. llythyr neu e-bost wedi'i anfon at y person anghywir sy'n cynnwys gwybodaeth bersonol)
  - Datgelu gwybodaeth bersonol amhriodol (e.e. ar lafar neu bostio gwybodaeth yn wallus ar wefan y Cyngor)
  - Colli copi caled neu ffeil bapur sy'n cynnwys gwybodaeth bersonol
  - Maleiswedd (e.e. feirws) sydd wedi treiddio i rwydwaith y Cyngor

Penderfynu a yw'r alwad yn achos neu'n ddigwyddiad

Er mwyn penderfynu a ddylid trin galwad fel achos neu ddigwyddiad, bydd y Garfan Rheoli Gwybodaeth, y Garfan Seiberddiogelwch, neu'r ddau (gan ddibynnu ar natur y tor diogelwch), yn ystyried ffactorau megis:

- Sefydlu os oes tor wedi digwydd, neu os oes potensial i dor ddigwydd heb fesurau ataliol
- Sensitifrwydd yr wybodaeth sydd wedi'i heffeithio
- Nifer gwrthrychau'r data sydd wedi'u heffeithio
- Yr effaith bosibl ar wrthrychau'r data (e.e. risg i'w hawliau a'u rhyddid)
- Yr effaith bosibl ar y Cyngor
- Unrhyw gamau sydd wedi'u cymryd eisoes i atal neu wella'r sefyllfa.
- A oedd y data wedi'i amgryptio (mewn achosion o golled neu ladrad)
- P'un a oedd y datgeliad yn fewnol (rhwng gweithwyr y Cyngor) neu'n allanol (e.e. aelod o'r cyhoedd)

Os oes ansicrwydd ynghylch sut i ddosbarthu'r alwad, bydd y mater yn cael ei gyfeirio at y Grŵp Diogelwch Gwybodaeth am benderfyniad.

2. Mynd i'r afael â Digwyddiad Diogelwch Gwybodaeth

Bydd digwyddiadau diogelwch gwybodaeth yn cael eu cyfeirio at, ac yn cael eu trin gan, y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch, gan weithio'n uniongyrchol gyda'r rheolwr gwasanaeth perthnasol. Ar gyfer digwyddiadau sy'n cynnwys Aelodau Etholedig, y Swyddog Monitro fydd y pwynt cyswllt.

Caiff digwyddiadau eu cofnodi'n ffurfiol ond fel arfer maen nhw'n cael eu rheoli drwy gyngor ac arweiniad anffurfiol yn hytrach nag ymchwiliad llawn i achos. Nid oes angen adroddiad achos ar gyfer digwyddiadau. Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn rhoi cyngor i'r rheolwr (neu'r Swyddog Monitro, ar gyfer Aelodau Etholedig) mewn perthynas â chamau priodol er mwyn mynd i'r afael â'r digwyddiad, ac mae'r rheolwr yn gyfrifol am weithredu unrhyw gamau a argymhellir.

3. Mynd i'r afael ag Achos Seiberddiogelwch Gwybodaeth

Bydd achosion seiberddiogelwch yn cael eu trin yn unol â'r gweithdrefnau canlynol:

- Cynllun Ymateb i Achos Seiberddiogelwch
- Gweithdrefn TGCh ar gyfer delio ag Achos neu Ddigwyddiad Gwe-rwydo

4. Mynd i'r afael ag Achos Diogelwch Gwybodaeth

Bydd pob achos yn cael ei ymchwilio'n llawn er mwyn cadarnhau'r ffeithiau ac unrhyw gamau unioni/ataliol sydd eu hangen. Ni fydd pob achos yn gofyn am yr un math o ymchwiliad; bydd y dull yn gymesur â'r amgylchiadau a'r difrifoldeb. Diben yr ymchwiliad i'r achos yw:

- Cadarnhau'r ffeithiau a phenderfynu beth aeth o'i le – maint y tor, swm a sensitifrwydd yr wybodaeth dan sylw

- Nodi effaith a difrifoldeb posibl yr achos ar y Cyngor ac ar yr unigolion sydd wedi'u heffeithio (gan gynnwys asesu a oes risg uchel i’w hawliau a’u rhyddid, ac a oes angen rhoi gwybod iddyn nhw am yr achos).

- Nodi unrhyw botensial ar gyfer colled neu ddifrod i'r Cyngor neu unrhyw gorff arall.

- Nodi risgiau sy'n briodol ar gyfer camau dilynol a gweithredu i'w lliniaru.

- Gwneud argymhellion i fynd i'r afael â risgiau sy wedi'u nodi.

- Llywio prosesau busnes a chynllunio yn y dyfodol.

- Penderfynu a ddylid rhoi gwybod am yr achos i’r Comisiynydd Gwybodaeth (os yw’n ymwneud â data personol) ac/neu unrhyw gorff rheoleiddio arall.

Bydd y broses ymchwilio i achosion yn cael ei harwain gan y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch, ar y cyd â'r Pennaeth Gwasanaeth perthnasol. Yn dibynnu ar natur a difrifoldeb yr achos, mae modd i'r ymchwiliad gynnwys:

- Casglu a chofnodi gwybodaeth

- Cyfarfod â'r rhai sy'n rhan o'r achos

- Cymryd datganiadau, ffurfiol neu anffurfiol, gan y rhai sy'n rhan o'r achos gan gynnwys unrhyw dystion

- Ymgynghori neu ymgysylltu ag Adran Adnoddau Dynol, Archwilio Mewnol a / neu Wasanaethau Cyfreithiol y Cyngor

- Rhoi gwybod am yr achos i Swyddfa’r Comisiynydd Gwybodaeth lle mae toriad difrifol wedi’i nodi sy’n effeithio ar hawliau a rhyddid y sawl yr effeithir arnyn nhw

- Rhoi gwybod i’r unigolyn yr effeithir arnyn nhw (gwrthrychau data) lle nodwyd ei bod hi'n bosibl bod risg uchel i’w hawliau a’u rhyddid.

- Cynnwys Carfan y Wasg y Cyngor os yw'r achos wedi cael ei gyhoeddi neu'n debygol o gael ei gyhoeddi.

5. Achosion sy'n Ymwneud â Data Personol

Lle mae data personol yn cael ei effeithio gan achos, bydd y Garfan Rheoli Gwybodaeth yn cynnal asesiad i benderfynu a yw'n bodloni diffiniad tor diogelwch data personol y Rheoliadau Diogelu Data Cyffredinol.

Asesu Risg Tor Diogelwch Data Personol

Os caiff achos ei asesu fel tor diogelwch data personol, bydd asesiad risg yn cael ei gynnal gan y Swyddog Diogelu Data (neu swyddog dirprwyedig) ar ôl ymgynghori â'r Pennaeth Gwasanaeth perthnasol, i benderfynu ar yr effaith wirioneddol neu bosibl ar hawliau a rhyddid yr unigolion yr effeithir arnynt. **Rhaid** i hyn gael ei wneud cyn pen **72 awr** o ddod yn ymwybodol o'r toriad, er mwyn cydymffurfio â gofynion adrodd Swyddfa'r Comisiynydd Gwybodaeth.

Wrth asesu risg y tor diogelwch data personol, bydd y Swyddog Diogelu Data a Phennaeth y Gwasanaeth yn ystyried:

- Natur y toriad
- Nifer y gwrthrychau data sydd wedi'u heffeithio
- Categorïau'r gwrthrychau data sydd wedi'u heffeithio
- Maint y data sydd wedi'i heffeithio
- Categorïau'r data sydd wedi'i effeithio a'i sensitifrwydd
- Pa mor hawdd y gellir adnabod unigolion
- Mesurau a gymerwyd er mwyn cynnwys yr achos
- Canlyniadau / effeithiau andwyol posibl neu wirioneddol ar yr unigolion yr effeithiwyd arnynt gan yr achos, gan gynnwys:
    - Preifatrwydd
    - Materion ariannol personol
    - Difrod materol arall
    - Iechyd a diogelwch
    - Llesiant emosiynol
    - Difrod anfaterol arall

Rhoi gwybod am y Tor Diogelwch Data Personol i Swyddfa'r Comisiynydd Gwybodaeth.

Lle mae tor diogelwch yn debygol o arwain at risg i hawliau a rhyddid unigolion, bydd y Swyddog Diogelu Data yn cyfeirio'r tor diogelwch at yr Uwch Berchennog Risg Gwybodaeth neu swyddog dirprwyedig, ynghyd â'u cyngor a'u hargymhellion. Mae'r Uwch Berchennog Risg Gwybodaeth (neu swyddog dirprwyedig) yn gyfrifol am ystyried yr amgylchiadau a'r cyngor a ddarperir gan y Swyddog Diogelu Data, ac am wneud y penderfyniad ynghylch a ddylid adrodd am y toriad i Swyddfa'r Comisiynydd Gwybodaeth. Ni ddylai'r Swyddog Diogelu Data roi gwybod am y toriad i Swyddfa'r Comisiynydd Gwybodaeth oni bai a hyd

nes y rhoddir cyfarwyddyd penodol i wneud hynny gan yr Uwch Berchennog Risg Gwybodaeth neu swyddog dirprwyedig.

Wrth roi gwybod am dor diogelwch data i Swyddfa'r Comisiynydd Gwybodaeth, bydd y Swyddog Diogelu Data yn defnyddio ffurflen adrodd Swyddfa'r Comisiynydd Gwybodaeth ac yn darparu:

- Disgrifiad o natur y tor diogelwch data personol gan gynnwys, lle bo modd:
    - Y categorïau a nifer bras yr unigolion dan sylw
    - Y categorïau a nifer bras y cofnodion data personol dan sylw
- Enw a manylion cyswllt y Swyddog Diogelu Data neu bwynt cyswllt arall lle gellir cael rhagor o wybodaeth
- Disgrifiad o ganlyniadau tebygol y tor diogelwch data personol
- Disgrifiad o'r mesurau a gymerwyd, neu a gynigiwyd, i fynd i'r afael â'r tor diogelwch data personol a, lle bo'n briodol, y camau a gymerwyd i liniaru unrhyw effeithiau andwyol posibl

Rhaid adrodd am achosion o dorri rheolau sy'n gofyn am roi gwybod i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr i'r Cyngor ddod yn ymwybodol o'r toriad, oni bai bod rheswm clir a chyfiawn dros yr oedi. Rhaid i unrhyw oedi y tu hwnt i 72 awr gynnwys esboniad dros roi gwybod yn hwyr.

Hysbysu gwrthrychau data am dor diogelwch data personol

Os yw toriad yn debygol o arwain at risg uchel i hawliau a rhyddid unigolion, bydd y Cyngor yn hysbysu'r rhai yr effeithir arnynt yn uniongyrchol a heb oedi gormodol.

Mae'r cyfrifoldeb am hysbysu unigolion yn nwylo'r Gwasanaeth perthnasol, a rhaid iddo wneud hynny ar ôl ymgynghori â'r Garfan Rheoli Gwybodaeth. Bydd y Garfan Rheoli Gwybodaeth yn darparu cyngor a chymorth arbenigol i sicrhau bod hysbysiadau'n gywir, yn amserol, ac yn cydymffurfio â gofynion cyfreithiol.

Ni ddylid rhoi unrhyw hysbysiad i wrthrychau data oni bai a hyd nes y cytunir ar y dull gyda'r Garfan Rheoli Gwybodaeth.

6. Camau gweithredu ac argymhellion a nodwyd yn ystod ymchwiliad

Ar ôl i ymchwiliad achos ddod i ben, bydd camau gweithredu ac argymhellion yn cael eu nodi i liniaru risg achos o natur debyg yn digwydd eto yn y dyfodol cyn belled â phosibl. Rhaid cofnodi camau gweithredu ac argymhellion yn yr adroddiad ymchwiliad yr achos.

Bydd pob cam gweithredu yn derbyn dyddiad cwblhau, ac yn cael ei ddyrannu i swyddog cyfrifol. Rhaid i'r swyddog cyfrifol gadarnhau, drwy lofnodi'r adroddiad, ei ymrwymiad i gwblhau'r camau gweithredu o fewn yr amserlen benodedig. Cyfrifoldeb y swyddog penodedig yw sicrhau bod yr holl gamau gweithredu yn cael eu cwblhau yn unol ag adroddiad yr ymchwiliad ac erbyn y dyddiad cwblhau cytunedig.

Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn monitro camau gweithredu, gan ddibynnu ar natur y tor diogelwch data. Os na chwblheir y camau gweithredu o fewn yr amserlen y cytunwyd arni, gellir cyfeirio'r mater at y Bwrdd Rheoli Gwybodaeth a/neu'r Pennaeth Gwasanaeth neu'r Cyfarwyddwr Gwasanaeth perthnasol i'w adolygu a chymryd camau pellach.

Atodiad I: Llif Gwaith Cyfeirio Cyflym: Ymchwilio i Ddigwyddiadau ac Achosion yn ymwneud â Diogelwch Gwybodaeth

1. **Galwad Diogelwch wedi'i Chodi**
   - Bydd y Ddesg Gwasanaeth TGCh yn cofnodi'r alwad ac yn ei hanfon at y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch.

2. **Asesiad Cychwynnol**
   - Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn asesu natur y mater (e.e. seiberddiogelwch, tor diogelwch data personol).
   - Os yw data personol yn gysylltiedig, bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn ystyried a oes tor diogelwch data personol wedi digwydd.

3. **Dosbarthiad**
   - Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn dosbarthu'r alwad naill ai fel digwyddiad (toriad posibl/mewnol) neu achos (toriad gwirioneddol/tebygol gydag effaith).
   - Os oes ansicrwydd, bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn ymgynghori â'r Grŵp Diogelwch Gwybodaeth.

4. **Trin Digwyddiadau**
   - Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn rheoli'r digwyddiad gyda'r rheolwr perthnasol.
   - Rhoi cyngor/arweiniad; nid oes angen adroddiad achos ffurfiol.
   - Bydd y rheolwr yn gweithredu'r camau sydd wedi'u hargymell.
   -

5. **Ymdrin ag Achosion**
   - Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn arwain yr ymchwiliad gyda'r Pennaeth Gwasanaeth perthnasol.
   - Casglu tystiolaeth, cyfweld â phartïon dan sylw, ymgynghori â'r Adrannau Adnoddau Dynol/Cyfreithiol yn ôl yr angen.
   - Asesu effaith, nodi camau cywirol/ataliol.

6. **Tor Diogelwch Data Personol (os yn berthnasol)**
   - Bydd y Swyddog Diogelu Data (neu ddirprwy) yn cynnal asesiad risg cyn pen 72 awr.
   - Bydd y Swyddog Diogelu Data yn cyfeirio at yr Uwch Berchennog Risg Gwybodaeth neu swyddog dirprwyedig ar gyfer penderfyniad ynghylch adroddiadau Swyddfa'r Comisiynydd Gwybodaeth.

- Bydd Swyddog Diogelu Data ond yn rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth os byddan nhw'n derbyn cyfarwyddyd gan Uwch Berchennog Risg Gwybodaeth neu swyddog dirprwyedig i wneud hynny.
- Bydd y gwasanaeth yn hysbysu unigolion yr effeithir arnynt ar ôl ymgynghori â'r Garfan Rheoli Gwybodaeth.

7. Camau Gweithredu a Monitro

- Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn cofnodi camau gweithredu/argymhellion, yn neilltuo swyddog cyfrifol a dyddiad cau.
- Bydd perchnogion camau gweithredu (swyddogion cyfrifol) yn cwblhau camau gweithredu a neilltuwyd o fewn yr amserlen y cytunwyd arni.
- Bydd y Garfan Rheoli Gwybodaeth a/neu'r Garfan Seiberddiogelwch yn monitro cwblhad y gwaith; yn uwchgyfeirio camau gweithredu anghyflawn i'r Bwrdd Rheoli Gwybodaeth a/neu'r Pennaeth Gwasanaeth/Cyfarwyddwr Gwasanaeth perthnasol.

Rheoli'r fersiwn

Rhif y fersiwn	Dyddiad wedi'i gymeradwyo gan y Garfan Rheoli Gwybodaeth a'r Garfan Seiberddiogelwch	Yn ddilys o	Yn ddilys hyd at	Newidiadau wedi'u gwneud
1.0	10.08.2016	10.08.2016	10.08.2017	Gweithdrefn newydd wedi'i datblygu yn seiliedig ar bolisi blaenorol Ymchwilio i Ddigwyddiadau Gwybodaeth.
1.1	11.08.2017	11.08.2017	01.10.2019	Adolygwyd gan y Garfan Rheoli Gwybodaeth – dim newidiadau
1.2	02.10.2019	02.10.2019	27.11.2022	Gofynion adrodd diwygiedig Swyddfa'r Comisiynydd Gwybodaeth, teitlau swyddi ac amserlenni/prosesau ar gyfer achosion/digwyddiadau i adlewyrchu arferion gwaith cyfredol.
1.3	28.11.2022	28.11.2022	12.11.2024	Adolygwyd. Rhifau'r adrannau a'r dudalen gynnwys wedi'u diweddaru.
1.4	13.11.2024	13.11.2024	21.10.2025	
1.5	22.10.2025	22.10.2025		Adolygiad a diweddariad cyffredinol. Wedi ychwanegu cyfeiriad at y Garfan Seiberddiogelwch. Penderfyniad achos/digwyddiad – wedi'i newid i ymgynghori â'r Grŵp Diogelwch i wneud penderfyniad yn hytrach na'r Swyddog Diogelu Data. Digwyddiadau – cyfeirio at Bennaeth y Gwasanaeth yn lle'r Hyrwyddwr Rheoli Gwybodaeth. Dogfen Visio wedi'i disodli gan lif gwaith cyfeirio cyflym.