Y Polisi Diogelwch Gwybodaeth

Mae'r polisi hwn yn amlinellu'r egwyddorion allweddol i sicrhau bod ein gwybodaeth yn cael ei chadw'n ddiogel, gan roi sylw i faterion fel diogelwch y swyddfa; trin, trosglwyddo a rhannu gwybodaeth; a sut mae rhoi gwybod am achosion posibl o dorri diogelwch data.

Statws y ddogfen: Cymeradwywyd
Fersiwn: 4
Dyddiad cymeradwyo: 30 Ionawr 2024
Yn weithredol o: Chwefror 2024
Perchennog: Uwch-berchennog Risg Gwybodaeth
Awdur: Swyddog Llywodraethu Gwybodaeth
Dyddiad adolygu nesaf arfaethedig: Chwefror 2027

Cynnwys

1. Diogelwch y swyddfa – Allweddi mynediad i'r swyddfa

1.1 Mae cyflogeion, aelodau, gweithwyr, contractwyr a'r rheini sy'n gweithio ar ein rhan yn gyfrifol am sicrhau nad oes neb yn cael mynediad heb awdurdod a bod ein hadeiladau'n cael eu gadael yn ddiogel. Mae hyn yn cynnwys sicrhau bod drysau yn cael eu cau, bod unigolion dieithr yn cael eu herio, a bod ymwelwyr yn cael eu hebrwng.

1.2 Yr Adran Cyfleusterau sy'n gyfrifol am sicrhau bod cofnod yn cael ei wneud o'r holl allweddi mynediad a roddir i weithwyr a/neu aelodau, a bod yr allweddi hynny wedi'u ffurfweddu ar gyfer pob unigolyn, ar sail eu gofynion mynediad.

1.3 Ni ddylai cyflogeion, aelodau, contractwyr na gweithwyr gael mynediad yn awtomatig i bob man yn y swyddfa, yn enwedig ardaloedd sensitif fel ystafell y gweinydd.

2. Diogelwch y swyddfa – Bathodynnau adnabod (ID)

2.1 Mae'n rhaid i gyflogeion, aelodau, gweithwyr, contractwyr ac ymwelwyr wisgo bathodyn adnabod a laniard bob amser pan fyddant ar ein safle.

2.2 Mae'n rhaid i bob cyflogai, aelod, gweithiwr, contractwr ac ymwelydd fod yn ymwybodol o'r gofyniad gan yr adrannau AD a Chyfleusterau i arddangos eu bathodyn bob amser.

2.3 Bydd cyflogeion, aelodau, gweithwyr, contractwyr ac ymwelwyr yn cael un o'r laniardiau canlynol:

- Laniard glas ar gyfer cyflogeion,
- Laniard gwyrdd ar gyfer aelodau, a
- Laniard coch ar gyfer ymwelwyr.

Ni cheir defnyddio mathau eraill o laniardau.

2.4 Dylai cyflogeion ac aelodau herio unigolion sydd heb fathodyn ID amlwg. Anogir pob cyflogai i ddilyn yr arfer da hwn neu, o leiaf, i roi gwybod i'r Rheolwr Cyfleusterau neu'r Tîm Llywodraethu am unigolion sydd heb fathodyn ID.

2.5 Disgwylir i aelodau wisgo eu bathodynnau ID wrth ymgymryd â'u rôl gyda'r Cyngor Optegol Cyffredinol yn ein swyddfeydd ac mewn lleoliadau allanol, er enghraifft, wrth ymweld â darparwyr addysg ac mewn gwrandawiadau.

2.6 Bydd y Tîm Cyfleusterau yn cadw cofrestr o fathodynnau ID ar gyfer pob gweithiwr ac aelod. Bydd y gofrestr yn nodi'r dyddiad cyhoeddi, unrhyw fathodynnau coll neu fathodynnau sydd wedi'u difrodi. Rhaid i'r Tîm Cyfleusterau drefnu bod staff newydd yn cael bathodynnau ID cyn ymuno â'r Cyngor Optegol Cyffredinol. Caiff y bathodynnau eu rhoi fel rhan o'r broses gynefino o fewn y pum niwrnod cyntaf ar ôl ymuno.

2.7 Rhaid i staff newydd sy'n gweithio yn y swyddfa gael bathodyn ymwelydd bob dydd gan y Tîm Cyfleusterau hyd nes eu bod yn cael eu bathodyn ID swyddogol.

2.8 Os bydd cyflogai, aelod, gweithiwr neu gontractwr yn newid ei swydd, rhaid i'r tîm Cyfleusterau/Llywodraethu sicrhau bod bathodyn ID newydd yn cael ei roi ar ddiwrnod cyntaf y rôl newydd a bod yr hen un yn cael ei ddychwelyd, ei gofnodi a'i waredu'n ddiogel.

2.9 Rhaid i gyflogeion ddychwelyd eu bathodyn ID i'r adran Adnoddau Dynol ar ddiwrnod olaf eu gwasanaeth. Rhaid i aelodau, gweithwyr a chontractwyr ddychwelyd eu bathodynnau ID yn ystod eu hwythnos olaf. Bydd y Tîm Cyfleusterau yn gwaredu'r bathodyn ID yn ddiogel ac yn cofnodi hynny.

3. Rhoi Gwybod os yw Bathodyn ID neu Allwedd wedi Mynd ar Goll neu Wedi'u Dwyn

3.1 Rhaid i gyflogeion, aelodau, gweithwyr neu gontractwyr roi gwybod i'r Tîm Cyfleusterau a'r Swyddog Llywodraethu Gwybodaeth ar unwaith os ydynt wedi colli eu bathodyn ID neu Allwedd Mynediad neu os cawsant eu dwyn.

3.2 Bydd y Tîm Cyfleusterau yn analluogi allwedd mynediad yr unigolyn ar unwaith. Mae'r Cyngor Optegol Cyffredinol yn cadw'r hawl i godi £20 ar unigolion os ydynt yn colli allwedd mynediad.

3.3 Bydd y Tîm Cyfleusterau yn cofnodi bod y bathodyn ID ar goll ac yn rhoi bathodyn arall yn ei le.

3.4 Gan y bydd angen i'r unigolyn roi gwybod bod bathodyn/allwedd wedi mynd ar goll cyn cael un newydd, nid oes rhaid llenwi ffurflen cofnodi digwyddiad diogelwch heblaw bod yna achos gwirioneddol o dorri diogelwch data (e.e. mynediad heb awdurdod i'r eiddo) neu os yw'r unigolyn wedi methu â rhoi gwybod bod ei fathodyn/allwedd ar goll.

4. Ymwelwyr

4.1 Dylid hysbysu'r dderbynfa drwy e-bost o leiaf 24 awr ymlaen llaw am unrhyw ymwelwyr.

4.2 Rhaid i ymwelwyr fynd i'r dderbynfa ar ôl cyrraedd a llenwi'r wybodaeth yn y llyfr ymwelwyr. Caiff y llyfr ei storio allan o'r golwg.

4.3 Bydd ymwelwyr yn cael bathodyn ymwelydd a laniard coch. Rhaid eu gwisgo'n weladwy bob amser pan fyddan nhw ar safle'r Cyngor Optegol Cyffredinol.

4.4 Rhaid i ymwelwyr nad ydynt yn gweithio ar ran y Cyngor Optegol Cyffredinol (sydd heb lofnodi cytundeb peidio â datgelu neu gytundeb cyfrinachedd) gael eu casglu o'r dderbynfa gan y cyflogai sy'n eu derbyn a'u hebrwng o amgylch y swyddfa yr holl

amser. Ni ddylid byth eu gadael heb oruchwyliaeth, ac eithrio yn ardal y dderbynfa ac ardaloedd cyhoeddus.

4.5 Lle nad yw'n bosibl aros gyda'r ymwelwyr yr holl amser, rhaid i bob cyflogai fod yn ymwybodol o ble mae'r ymwelydd yn gweithio a phwrpas yr ymweliad.

4.6 Rhaid i ymwelwyr ddychwelyd eu bathodyn a'u laniard, a llenwi'r manylion gadael yn y llyfr ymwelwyr wrth adael ein safle.

5. Trin gwybodaeth

5.1 Mae'r adran hon yn egluro sut rydym yn trin gwybodaeth yn ddiogel. Mae'n cynnwys ein dulliau gweithredu ar gyfer:

- Storio Gwybodaeth (gan gynnwys Desg Glir a Sgrin Glir);
- Argraffu;
- Gwaredu; a
- Thempledi.

5.2 I gael rhagor o fanylion am y prosesau hyn, trwoch at y canllawiau gweithredol, cyfarwyddiadau lleol neu'r polisïau cysylltiedig.

5.3 Dylai pob cyflogai, aelod, gweithiwr, contractwr a phawb sy'n gweithio ar ein rhan drin unrhyw wybodaeth fel y byddent yn dymuno bod eraill yn trin eu gwybodaeth nhw.

5.4 Ni ddylai gwybodaeth bersonol (gan gynnwys gwybodaeth sensitif o safbwynt busnes) gael ei rhannu na'i datgelu gan gyflogeion a'r rheini sy'n gweithio ar ein rhan mewn modd heb ganiatâd mewn unrhyw fformat.

5.4 Rhaid i'r holl wybodaeth gyfrinachol, gwybodaeth bersonol neu wybodaeth categori arbennig, ar ffurf copi caled neu electronig, gael eu trin yn ddiogel er mwyn lliniaru'r risg o fynediad heb awdurdod.

Storio Gwybodaeth – Desg glir, sgrin glir, cloi gweithfan

5.5 Yn ystod y dydd, os nad oes neb yn eistedd tu ôl i ddesg, rhaid cadw dogfennau sy'n cynnwys gwybodaeth gyfrinachol, gwybodaeth bersonol neu wybodaeth categori arbennig mewn cwpwrdd neu ddrôr.

5.6 Rhaid cau a chloi unrhyw gwpwrdd neu ddrôr sy'n cynnwys gwybodaeth gyfrinachol, gwybodaeth bersonol neu wybodaeth categori arbennig pan nad ydynt yn cael eu defnyddio. Rhaid dychwelyd allweddi cypyrddau diogel i'r man storio allweddi ac ni ddylid eu gadael heb oruchwyliaeth.

5.7 Rhaid i unrhyw ddyfeisiau (e.e. cof bach, ffyn USB, DVDs) a dogfennau sy'n cynnwys gwybodaeth gyfrinachol, gwybodaeth bersonol neu wybodaeth categori arbennig gael eu clirio o'r desgiau ar ddiwedd pob diwrnod gwaith a'u cadw'n ddiogel.

5.8 Rhaid i gyfrifiaduron gael eu 'cloi' os nad oes neb wrth y ddesg a dylid eu diffodd ar ddiwedd y diwrnod gwaith.

5.9 Rhaid gofalu bod y wybodaeth sy'n cael ei harddangos ar bob dyfais electronig yn cael ei chadw'n gyfrinachol, yn enwedig mewn mannau cyhoeddus neu ar drafnidiaeth gyhoeddus.

Argraffu

5.10 Wrth argraffu gwybodaeth gyfrinachol, gwybodaeth bersonol neu wybodaeth categori arbennig, rhaid defnyddio'r opsiwn 'clo argraffu', a rhaid i'r unigolyn sy'n argraffu fod yna wrth yr argraffydd.

5.11 Rhaid casglu unrhyw bapurau o beiriannau argraffu cyn gynted ag y cânt eu hargraffu i sicrhau nad oes dogfennau cyfrinachol, personol neu gategori arbennig yn cael eu gadael yn nrôr yr argraffydd.

Gwaredu

5.12 Rhaid i ddogfennau cyfrinachol, personol neu gategori arbennig gael eu gwaredu'n ddiogel mewn biniau gwastraff cyfrinachol pan nad oes eu hangen mwyach. Dylid cymryd gofal i sicrhau bod y dogfennau'n cael eu rhoi i mewn i gyd ac nad oes modd eu hadfer o'r biniau.

5.13 Ar ddiwedd pob cyfarfod, rhaid clirio'r ystafelloedd ar unwaith o unrhyw ddogfennau sy'n cynnwys data cyfrinachol, data personol neu ddata categori arbennig. Mae hyn yn cynnwys glanhau byrddau gwyn a gwaredu siartiau troi.

5.14 I gael rhagor o wybodaeth am waredu gwybodaeth sydd wedi'i harchifo, darllenwch ein Polisi Diogelu Data.

Templedi

5.15 Rhaid i unrhyw dempledi a ddefnyddir fod yn wag. Ni ddylid defnyddio fersiynau o dempledi a ddiwygiwyd yn flaenorol fel y templed sylfaenol, oherwydd y risg y gallai gwybodaeth bersonol ymddangos y tro nesaf y caiff ei ddefnyddio.

6. Trosglwyddo a Rhannu Gwybodaeth yn Ddiogel

6.1 Mae'r adran hon yn ymwneud â sut i drosglwyddo data'n ddiogel. I gael rhagor o wybodaeth am pryd i rannu a phryd i beidio â rhannu gwybodaeth, darllenwch ein Polisi Diogelu Data a'n Polisi Datgelu.

6.2 Rhaid sicrhau bob amser bod lefel y diogelwch yn briodol i natur y data sy'n cael ei drosglwyddo.

Cludo / symud o gwmpas

6.3 Rhaid bod yn ofalus bob amser i sicrhau bod yr holl wybodaeth electronig a ffisegol yn cael ei chludo'n ddiogel. Mae hyn yn cynnwys sicrhau bod gliniaduron wedi'u diffodd pan fyddant yn cael eu cludo fel bod dal angen y cod amgryptio i'w hagor a chymryd y camau priodol fel rhoi dogfennau sensitif mewn ffeil y gellir ei chloi.

Postio

6.4 Rhaid i'r anfonwr wirio pob post cyn ei anfon. Rhaid i'r gwiriad hwn gynnwys:

- cymharu'r cyfeiriad ar yr amlen a'r llythyr â'r cyfeiriad a gedwir ar ffeil;
- sicrhau mai'r wybodaeth sydd wedi'i chynnwys yw'r wybodaeth gywir ar gyfer y derbynnydd;
- bod pob darn perthnasol wedi'i ddileu/guddio'n llawn a bod person arall wedi dilysu hyn; ac
- nad oes unrhyw wybodaeth bellach wedi'i chynnwys, o ganlyniad i wall wrth argraffu, sganio neu ddefnyddio templed er enghraifft.

6.5 Mae'r Tîm Cyfleusterau wedi creu taenlenni postio i gofnodi post sy'n dod i mewn ac allan. Rhaid llenwi'r daenlen bob tro y byddwch yn anfon neu'n derbyn unrhyw bost.

6.6 Wrth bostio gwybodaeth gyfrinachol, gwybodaeth bersonol neu wybodaeth categori arbennig, defnyddiwch amlenni sydd ddim yn rhwygo neu amlenni dwbl (gan sicrhau bod yr enw a'r cyfeiriad ar y ddwy amlen), marciwch nhw'n 'preifat a chyfrinachol' neu 'ar gyfer y derbynnydd yn unig', a'u hanfon drwy bost cofrestredig neu gwmni cludo.

6.7 Er mwyn hwyluso'r gwaith o reoli'r busnes yn briodol, fel egwyddor gyffredinol, gall y Tîm Cyfleusterau agor unrhyw bost a dderbyniwn yn y Cyngor Optegol Cyffredinol er mwyn sefydlu pwy yw'r derbynnydd arfaethedig a phriodol os yw wedi cael ei gyfeirio'n rhesymol at y Cyngor Optegol Cyffredinol.

6.8 Os yw post wedi'i farcio'n 'preifat a chyfrinachol neu 'ar gyfer y derbynnydd yn unig', ac wedi'i gyfeirio at y Cyngor Optegol Cyffredinol, bydd yn cael ei roi i'r Rheolwr Cyfleusterau i'w agor, i'w lofnodi a'i gofnodi. Yn absenoldeb y Rheolwr Cyfleusterau, bydd ein tîm Cyfleusterau yn gofyn caniatâd y Pennaeth Cyllid neu'r Pennaeth Llywodraethu.

Negeseuon e-bost

6.9 Rhaid i'r anfonwr wirio pob e-bost cyn ei anfon. Rhaid i'r gwiriad hwn gynnwys:

- sicrhau bod y cyfeiriad e-bost yn gywir (gellid anfon e-bost prawf yn gyntaf os oes angen);
- sicrhau mai'r wybodaeth sydd wedi'i chynnwys yw'r wybodaeth gywir ar gyfer y derbynnydd;
- bod pob darn perthnasol wedi'i ddileu/guddio'n llawn a bod person arall wedi dilysu hyn; ac

- nad oes unrhyw wybodaeth bellach wedi'i chynnwys, o ganlyniad i wall wrth argraffu, wrth ddefnyddio templed, neu yn nhrywydd blaenorol y neges er enghraifft.

6.10 Wrth anfon negeseuon e-bost, mae'n bwysig ystyried:

- pwy yw'r derbynnydd/derbynwyr, a ydynt yn fewnol/allanol;
- os yw'n dderbynnydd allanol, a allai'r neges gael ei rhyng-gipio;
- ydy'r e-byst blaenorol yn yr ohebiaeth yn dal yn berthnasol;
- a oes angen cyfrinair neu a oes angen amgryptio atodiadau;

a/neu;

- marc diogelwch ar yr e-bost.
- pan fydd sawl derbynnydd, defnyddiwch y maes "bcc/cudd" i guddio cyfeiriadau e-bost.

6.11 Fel mesur diogelwch ychwanegol, dylai anfonwyr ystyried diffodd awto-lenwi cyfeiriadau e-bost yn Outlook. Gall Perchnogion Asedau Gwybodaeth wneud y dewis hwn yn orfodol.

6.12 Dylai anfonwyr hefyd ystyried cynnwys marciau diogelwch ym mhwnc a chorff yr e-bost ac fel gosodiad yr e-bost, fel y bo'n briodol.

6.13 I gael rhagor o wybodaeth am fesurau diogelwch electronig, darllenwch y Polisi TG.

Ar lafar/dros y ffôn

6.14 Dylai defnyddwyr sicrhau nad oes neb yn gallu edrych dros eu hysgwydd na bod pobl eraill o fewn clyw os ydynt yn gweithio ar fusnes y Cyngor Optegol Cyffredinol neu'n ei drafod yn gyhoeddus.

6.15 Gall galwadau ffôn yn aml arwain at ddefnyddio neu ddatgelu data personol heb awdurdod. Mae'n rhaid cwblhau'r gwiriadau canlynol cyn rhyddhau'r data:

- Cadarnhau pwy yw'r galwr – drwy ofyn cwestiynau mai dim ond nhw fyddai'n gwybod yr ateb iddynt, neu drwy anfon e-bost neu eu ffonio'n ôl ar y manylion cyswllt sydd gennym ar ein system TG.
- Os nad nhw yw gwrthrych y data a'u bod yn gofyn am fanylion rhywun arall, ni ddylech ddatgelu gwybodaeth sy'n ymwneud â gwrthrych y data, oni bai eich bod wedi cael caniatâd penodol gan wrthrych y data. Mae gan wrthrych y data bob amser hawl i dynnu ei ganiatâd yn ôl ar unrhyw adeg drwy ysgrifennu at y Cyngor Optegol Cyffredinol. Os nad ydych yn siŵr, gofynnwch iddynt wneud eu cais yn ysgrifenedig, neu gymryd enw a rhif cyswllt a cheisio cyngor pellach gan y Swyddog Llywodraethu Gwybodaeth neu eich rheolwr llinell.

7. Cyfryngau cludadwy

7.1 Rydym yn cydnabod bod nifer o risgiau'n gysylltiedig â thrin gwybodaeth, yn enwedig o safbwynt defnyddio cyfryngau cludadwy, wrth gyflawni ein swyddogaethau. Am y rheswm hwn, ni chaniateir defnyddio dyfeisiau cyfryngau cludadwy oni bai fod cais dilys sy'n cyfiawnhau defnydd busnes dilys, bod hynny'n drech na'r risgiau a'r gwendidau cysylltiedig, a bod y cais wedi'i gymeradwyo yn unol â'r Polisi a'r broses TG.

7.2 Mae cyfryngau cludadwy yn cynnwys y canlynol, ymhlith eraill: Cardiau cyfryngau; CDs; DVDs; gyriannau caled allanol; cof bach USB; unrhyw ddyfeisiau storio electronig eraill.

7.3 Rhaid trin cyfryngau cludadwy fel gwybodaeth gyfrinachol, gwybodaeth bersonol, neu wybodaeth categori arbennig a hynny'n unol â'r Polisi Diogelu Data.

7.4 Ein hadran TG sy'n rheoli'r broses ar gyfer cael gafael ar gyfryngau cludadwy a'r defnydd ohonynt. Rhaid i unigolion ystyried trefniadau amgen, mwy diogel, cyn gofyn am gael defnyddio cyfryngau cludadwy.

7.5 Os ydych chi'n defnyddio dyfeisiau cyfryngau cludadwy i drosglwyddo data, rhaid i chi ystyried y ffordd fwyaf priodol o gludo'r ddyfais a dangos eich bod wedi cymryd gofal rhesymol i osgoi difrod neu golled, gan gynnwys amgryptio'r ddyfais.

7.6 Dim ond dyfeisiau cyfryngau cludadwy a gyflenwir gan ein tîm TG y gellir eu defnyddio. Ni ddylid defnyddio dyfeisiau cyfryngau cludadwy personol (nad ydynt yn eiddo i'r Cyngor Optegol Cyffredinol) i storio unrhyw wybodaeth am y busnes ac ni ddylid defnyddio dyfeisiau o'r fath gydag unrhyw offer sy'n eiddo i'r Cyngor Optegol Cyffredinol.

7.7 Ni ddylid defnyddio cyfryngau cludadwy a ddarperir gan y Cyngor Optegol Cyffredinol at unrhyw bwrpas heblaw'r diben cymeradwy. Dim ond data sydd wedi'i awdurdodi ac sy'n angenrheidiol i'w drosglwyddo y dylid ei gadw ar ddyfais cyfryngau cludadwy.

7.8 Ni ddylid defnyddio dyfeisiau cyfryngau cludadwy ar gyfer archifo na storio cofnodion yn lle defnyddio rhwydwaith y Cyngor Optegol Cyffredinol.

7.9 Rhaid rhoi dyfeisiau cyfryngau cludadwy yn ôl i wrthrych y data pan nad oes angen eu cadw mwyach ar y busnes. Os nad yw gwrthrych y data yn dweud ei fod eisiau'r ddyfais yn ôl, bydd yn cael ei ddinistrio yn unol â'n polisi Cadw Data ac Amserlenni.

Amgryptio

7.9 Rhaid amgryptio'r holl ddata sy'n cael ei storio ar gyfryngau cludadwy yn unol â safonau amgryptio y Cyngor Optegol Cyffredinol, fel a ddarperir gan TG.

7.10 Wrth ddefnyddio dyfais cyfryngau cludadwy i drosglwyddo data i drydydd parti, rhaid defnyddio dyfais wedi'i hamgryptio a ddarparwyd gan y Cyngor Optegol Cyffredinol.

7.11 Rhaid bod meddalwedd chwilio am feirysau a maleiswedd a gymeradwyir gan TG ar y peiriant y cymerir y data ohono ac ar y ddyfais fydd yn derbyn y data.

8. Rhoi gwybod am achos o dorri diogelwch gwybodaeth neu achos fu bron â digwydd

8.1 Disgwylir i bob cyflogai, aelod, gweithiwr, contractwr ac unigolyn sy'n gweithio ar ein rhan roi gwybod ar unwaith am achosion gwirioneddol, amheuaeth o achosion neu achosion posibl o dorri diogelwch gwybodaeth. Yn syth ar ôl darganfod y digwyddiad, rhaid i'r unigolyn hwnnw roi gwybod i'w reolwr llinell (neu reolwr llinell arall os nad yw ei reolwr ar gael), y Swyddog Llywodraethu Gwybodaeth a'i gyfarwyddwr, yn ogystal ag IG@optical.org.

8.2 Yn dibynnu ar natur y digwyddiad, efallai y bydd angen hysbysu'r unigolion neu'r bobl ganlynol hefyd er mwyn gallu rheoli'r mater yn gyflym ac yn briodol:

Math o ddigwyddiad	Rhoi gwybod i'r	Enghreifftiau
TG / Seiber	Cyfarwyddwr Gwasanaethau Corfforaethol a TG	Firysau, ymgais gwe-rwydo, gliniaduron, iPads neu ffonau symudol coll, cyfrineiriau a ddatgelwyd.
Diogelwch ffisegol	Rheolwr Cyfleusterau	Achosion o dorri diogelwch ffisegol – mynediad heb awdurdod ar y safle, allwedd mynediad coll.

8.3 Gallai hyn arwain at roi'r Cynllun Parhad Busnes ar waith neu bolisïau eraill.

8.4 O fewn 24 awr i ddod yn ymwybodol o'r digwyddiad, rhaid i'r hysbyswr gyflwyno ffurflen i roi gwybod am ddigwyddiad diogelwch. Dylid anfon y ffurflen hon ymlaen at y Swyddog Llywodraethu Gwybodaeth. Gall peidio â rhoi gwybod o fewn yr amserlen hon gael ei ystyried yn drosedd disgyblu.

8.5 Mae hyn yn bwysig oherwydd os yw'r digwyddiad yn risg uchel, efallai y bydd angen rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth o fewn 72 awr i'r adeg pan fydd rhywun (yr hysbyswr, trydydd parti, ac ati) yn dod yn ymwybodol am y tro cyntaf o'r digwyddiad.

8.6 Bydd angen i'r Swyddog Llywodraethu Gwybodaeth neu reolwr yr adran gwblhau ymchwiliad i'r digwyddiad. Os yw'r digwyddiad yn un difrifol, gellir ystyried cynnal ymchwiliad llawn yn unol â'n Polisi Ymchwilio mewnol.

8.7 Disgwylir i unrhyw reolwr sy'n cael gwybod am y tor-ddiogelwch yn unol â'r polisi hwn wneud pob ymdrech i leihau'r effaith, mewn cydweithrediad â'r Swyddog Llywodraethu Gwybodaeth.

8.8 Bydd y Swyddog Llywodraethu Gwybodaeth yn sicrhau bod y camau canlynol o reoli tor-ddiogelwch yn cael eu cwblhau'n brydlon, gan ystyried canllawiau Swyddfa'r Comisiynydd Gwybodaeth ar reoli achosion o dorri diogelwch:

- cyfyngu ac adfer;
- asesu'r risg barhaus;
- hysbysu am y tramgwydd; a;
- gwerthuso ac ymateb.

8.9 Bydd yr holl Adroddiadau am Ddigwyddiadau Diogelwch yn cael eu llofnodi gan y Swyddog Diogelu Data neu ei ddirprwy ar ôl cwblhau ymchwiliad.

8.10 Bydd y Swyddog Diogelu Data yn penderfynu a oes angen rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am unrhyw dramgwydd, gan ystyried canllawiau Swyddfa'r Comisiynydd Gwybodaeth, a bydd yn goruchwylio'r gwaith adrodd, lle bo angen. Mae angen rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth cyn pen 72 awr ar ôl dod yn ymwybodol o unrhyw achosion o dorri diogelwch sy'n berthnasol i Swyddfa'r Comisiynydd Gwybodaeth. Os na wnewch chi hyn, gall arwain at ddirwy awtomatig gan Swyddfa'r Comisiynydd Gwybodaeth.

8.11 Bydd yr adran(nau) priodol yn rhoi mesurau adferol a pharhaol ar waith i liniaru'r risg o ail-ddigwyddiad tebyg a byddant yn cael eu cefnogi gan y Swyddog Llywodraethu Gwybodaeth.

8.12 Bydd y Swyddog Llywodraethu Gwybodaeth yn cofnodi'r holl gamau a gymerwyd a'r gwersi a ddysgwyd o'r digwyddiad neu'r digwyddiadau y bu ond y dim iddynt ddigwydd, a bydd yn sicrhau bod y rhain yn cael eu rhannu â'r sefydliad bob hyn a hyn ar gyfer codi ymwybyddiaeth a dysgu parhaus.