Ombwdsmon
Ombudsman
Cymru • Wales

Polisi Diogelwch Gwybodaeth

Cynnwys

1. Pwrpas 3
2. Cwmpas 3
3. Amcanion diogelwch gwybodaeth 4
4. Byrfoddau 4
5. Rolau a dyletswyddau 5
6. Rheol Risg 6
7. Diogewlch Adnoddau Dynol 6
8. Rheoli Asedau 8
9. Rheoli rhwydwaith 9
10. Rheoli gwendidau 11
11. Diogelwch ffisegol ac amgylcheddol 12
12. Hunaniaeth a rheoli mynediad 15
13. Rheoli Digwyddiadau Diogelwch Gwybodaeth 15
14. Diogelwch yn y gadwyn gyflenwi 16
15. Monitro ac Adrodd 16
16. Adolygu 17
17. Polisi / proses / canllawiau cysylltiedig 17

1. Pwrpas

1.1. O dan ddeddfwriaeth diogelu data, rhaid i Ombwdsmon Gwasanaethau Cyhoeddus Cymru (OGCC) sicrhau bod ganddo reolaethau diogelwch technegol a sefydliadol priodol ar waith i ddiogelu data personol rhag prosesu diawdurdod neu anghyfreithlon a cholled, dinistr neu ddifrod damweiniol.

1.2. Mae gwerth i'r holl wybodaeth, gan gynnwys data personol, ac mae'n bwysig bod OGCC yn deall pa wybodaeth mae'n ei phrosesu i ystyried y ffordd orau o'i diogelu er mwyn sicrhau bod yr wybodaeth yn cael ei gwarchod pan fydd yn cael ei throsglwyddo neu ei chadw.

1.3. Yn gyffredinol, mae prosesu'n golygu casglu, defnyddio, datgelu, rhannu, cadw neu gael gwared ar ddata neu wybodaeth bersonol.

1.4. Gall digwyddiadau diogelwch gwybodaeth achosi niwed a thrallod i'r rheini y mae eu data personol mewn perygl. Ar gyfer OGCC, ceir risgiau cyfreithiol, ariannol ac i enw da.

1.5. Mae'r polisi hwn yn elfen allweddol o fframwaith llywodraethu gwybodaeth cyffredinol yr Ombwdsmon ac felly dylid ei ddarllen ar y cyd â pholisïau, gweithdrefnau a chanllawiau perthnasol y sefydliad.

2. Cwmpas

2.1. Mae'r polisi hwn yn ymwneud â'r holl wybodaeth, systemau gwybodaeth, rhwydweithiau, rhaglenni, lleoliadau a defnyddwyr gwasanaethau'r Ombwdsmon neu a gyflenwir o dan gontract iddo.

2.2. Mae'r polisi'n berthnasol i holl staff OGCC (gan gynnwys staff parhaol, staff contract, staff dros dro) ac unigolion neu sefydliadau sy'n cael eu contractio'n uniongyrchol gan OGCC).

3. Amcanion diogelwch gwybodaeth

Mae OGCC wedi ymrwymo i sicrhau'r lefel briodol o gyfrinachedd, uniondeb ac argaeledd asedau gwybodaeth ac i gynnal cadernid gweithgareddau hanfodol. Mae'r polisi hwn yn disgrifio egwyddorion diogelwch gwybodaeth ac yn egluro sut y byddan nhw'n cael eu rhoi ar waith yn y sefydliad. Mae'r polisi'n nodi sut y bydd OGCC yn gwneud y canlynol:

- Sicrhau bod pob aelod o staff yn ymwybodol o'r angen am ddiogelwch gwybodaeth mewn busnes o ddydd i ddydd, eu bod yn deall eu cyfrifoldebau a'u bod yn cydymffurfio'n gyson ac yn llawn â'r ddeddfwriaeth berthnasol fel y disgrifir yn y polisi hwn ac mewn polisïau eraill.

- Diogelu asedau gwybodaeth sydd dan reolaeth y sefydliad, gan gynnwys wrth gydweithio â chyflenwyr.

- Creu hinsawdd sy'n lleihau achosion o dorri'r polisi hwn ond sy'n annog rhoi gwybod yn brydlon ac yn agored am unrhyw achosion o dorri amodau o'r fath.

4. Byrfoddau

COODOI	Prif Swyddog Gweithredol a Chyfarwyddwr Gwella. At ddibenion llywodraethu gwybodaeth, cyfeirir ato hefyd fel Prif Swyddog Diogelwch Gwybodaeth (CISO).
ITM	Rheolwr Technoleg Gwybodaeth.
CLADOI	Prif Gynghorydd Cyfreithiol a Chyfarwyddwr Ymchwiliadau (At ddibenion llywodraethu gwybodaeth y cyfeirir ato hefyd fel Uwch-berchennog Risg Gwybodaeth (SIRO).
IGM	Rheolwr Llywodraethu Gwybodaeth.

5. Rolau a chyfrifoldebau

5.1. Mae'r COODOI yn atebol i'r Ombwdsmon am lywodraethu gwybodaeth yn gyffredinol, gan gynnwys diogelwch gwybodaeth OGCC. Mae hyn yn cynnwys seiberddiogelwch a chadernid rhwydweithiau OGCC. Mae'r COODOI yn gweithio gydag eraill i gynghori'r Ombwdsmon a'r Tîm Rheoli ar y ffordd orau o reoli risg ar yr un pryd â manteisio ar dechnoleg i gyflawni amcanion strategol OGCC.

5.2. CLADoI yw Uwch Swyddog Cyfrifol y sefydliad sy'n gyfrifol am fonitro'r gwaith o reoli risg o ran gwybodaeth yn y sefydliad.

5.3. Mae'r cyfrifoldeb dros reoli a gweithredu'r polisi a'r gweithdrefnau cysylltiedig yn gorwedd gyda'r ITM a'r IGM sy'n atebol i'r CLADOI a'r COODOI.

5.4. Rhaid i'r aelod staff neu'r rheolwr roi gwybod am unrhyw achosion o dorri'r polisi i'r ITM neu'r IGM cyn gynted ag y bo modd ar ôl cael gwybod am y tor-amod.

5.5. Mae'r ITM a'r IGM yn gyfrifol am sicrhau bod pawb sydd â mynediad awdurdodedig at systemau TG OGCC yn ymwybodol o'r canlynol:

- Y polisïau diogelwch gwybodaeth sy'n berthnasol yn eu meysydd gwaith.
- Eu cyfrifoldebau personol o ran diogelu gwybodaeth.
- Sut i gael gafael ar gyngor ar faterion diogelwch gwybodaeth.

5.6. Bydd yr holl staff yn cydymffurfio â'r Polisi hwn a gweithdrefnau a chanllawiau cysylltiedig ar ddiogelwch gwybodaeth a restrir ar ddiwedd y ddogfen hon. Bydd pob aelod o staff yn gyfrifol yn unigol am ddiogelwch eu hamgylcheddau ffisegol lle caiff gwybodaeth ei phrosesu neu ei storio.

5.7. Rhaid i bob defnyddiwr system gydymffurfio â'r gofynion diogelwch sydd mewn grym ar hyn o bryd, a rhaid iddyn nhw hefyd sicrhau bod cyfrinachedd, cywirdeb ac argaeledd yr wybodaeth sy'n cael ei defnyddio ganddyn nhw'n cael eu cynnal i'r safon uchaf.

6. Rheoli Risg

6.1. Mae OGCC yn cydnabod bod ganddo gyfrifoldeb i reoli risgiau mewnol ac allanol fel elfen allweddol o lywodraethu corfforaethol da. Mae wedi ymrwymo i wreiddio rheoli risg yng ngweithrediadau dyddiol y sefydliad, o osod amcanion i gynllunio gwasanaethau a chyllid i brosesau adrannol. Mae'n credu y bydd rheoli risg yn effeithiol yn ei helpu i gyflawni ei amcanion corfforaethol. Mae'r Polisi Rheoli Risg yn nodi dull OGCC o reoli risg, gan gynnwys adnabod a thrin risgiau.

6.2. Mae hyn yn cynnwys nodi a meintioli risgiau diogelwch gwybodaeth o ran gwerth tybiedig yr ased, difrifoldeb yr effaith a'r tebygolrwydd y bydd pob categori o wybodaeth yn digwydd.

6.3. Bydd pob tîm yn nodi risg fel eitem sefydlog ar agendâu eu cyfarfodydd tîm.

7. Diogelwch Adnoddau Dynol

7.1. **Contractau cyflogaeth**

Rhaid rhoi sylw i ofynion diogelwch staff yn ystod y cam recriwtio a rhaid i bob contract cyflogaeth gynnwys cymal cyfrinachedd, sy'n cyfyngu ar ddatgelu gwybodaeth gyfrinachol a gafwyd yn ystod eu cyflogaeth gyda'r Ombwdsmon.

7.2. Proses staff newydd a staff sy'n gadael

Bydd staff newydd sy'n ymuno ag OGCC yn cael mynediad priodol at adeiladau a TG yn ôl gofynion eu rôl. Mae mynediad at adeiladau a TG yn cael ei ddiddymu pan fydd staff yn gadael OGCC. Mae'r broses staff newydd a staff sy'n gadael yn cael ei rheoli ar y cyd rhwng y Gwasanaethau Corfforaethol a'r Tîm TG.

7.3. Newid swydd

Mae angen rhoi gwybod i'r Gwasanaethau Corfforaethol a'r Tîm TG am unrhyw newidiadau yn swydd y staff er mwyn gallu adolygu hawliau mynediad ffisegol / TG.

7.4. Hyfforddiant ac ymwybyddiaeth

Mae pawb yn gyfrifol am ddiogelwch gwybodaeth. Mae strategaeth hyfforddi ar lywodraethu gwybodaeth yn nodi gofynion hyfforddi a datblygu llywodraethu gwybodaeth y staff. Mae'r strategaeth hefyd yn cynnwys cynllun cyfathrebu sy'n nodi'r prif negeseuon ar gyfer y flwyddyn i ddod. Mae hyfforddiant gloywi gorfodol yn cael ei nodi bob blwyddyn ac yn cael ei gynnwys yng nghynllun hyfforddi blynyddol y sefydliad.

Bydd hyfforddiant ymwybyddiaeth o ddiogelwch gwybodaeth, a manylion Safonau Ymddygiad Staff (sy'n cynnwys defnydd derbyniol o TG), yn cael eu cynnwys yn y broses gynefino staff. Bydd yr hyfforddiant hwn yn cynnwys dealltwriaeth o'r polisi hwn a sut mae'n berthnasol i weithgareddau gwaith o ddydd i ddydd.

8. Rheoli Asedau

8.1. Caiff asedau gwybodaeth eu catalogio yn ôl swyddogaethau busnes a'u rheoli drwy'r Gofrestr Asedau Gwybodaeth. Mae Perchnogion a Chynorthwywyr Asedau Gwybodaeth yn nodi, yn gweithredu ac yn cynnal rheolaethau rheoli risg ar gyfer asedau gwybodaeth y maent yn gyfrifol amdanynt. Mae rhestr o'r asedau gwybodaeth sydd i'w hadolygu yn cael ei nodi'n flynyddol.

8.2. **Parhad busnes a chynlluniau Adfer ar ôl Trychineb**

Bydd OGCC yn sicrhau bod asesiadau o'r effaith ar fusnes, parhad busnes a chynlluniau adfer ar ôl trychineb yn cael eu cynhyrchu ar gyfer yr holl wybodaeth, rhaglenni, systemau a rhwydweithiau hanfodol.

Rhaid i staff gadw deunydd sy'n ymwneud ag achosion yn y system rheoli achosion, a ffeiliau a chofnodion eraill i'r systemau perthnasol, neu i yriannau gweinydd neu fewnrwyd yr Hwb. Ni ddylai staff ddefnyddio storfa ffeiliau lleol ar fwrdd gwaith na disg caled eu cyfrifiaduron.

Ceir manylion am drefniadau wrth gefn TG yn y Polisi Llywodraethu TG. Manylir ar y trefniadau wrth gefn yn y Polisi Llywodraethu TG ac maen nhw'n cynnwys:

- Efelychu gweinydd ar y safle – ar gyfer adfer data yn y tymor byr os bydd gweinydd/rhaglen yn methu.
- Copi wrth gefn ar y safle
- Copi wrth gefn yn y cwmwl
- Trefniadau wrth gefn o systemau wedi'u lletya

Mae rhagor o wybodaeth ar gael hefyd yng Nghynllun Parhad Busnes y sefydliad.

8.3. Mae systemau wedi'u cynllunio fel bod modd eu harchifo'n ddiogel ac yn ddiogel yn unol â gofynion y Polisi Rheoli Cofnodion pan fydd cofnodion yn cyrraedd eu cyfnod cadw perthnasol.

9. Rheoli rhwydwaith

9.1. Mae rhwydwaith TG a chyfathrebu OGCC yn cael ei ddylunio, ei ffurfweddu, ei gynnal a'i reoli gan y Tîm TG ar y cyd â'r Darparwr Gwasanaeth Cymorth TG. Maen nhw'n goruchwylio'r gwaith o redeg y rhwydwaith o ddydd i ddydd, gan sicrhau diogelwch, cyfrinachedd, cywirdeb ac argaeledd data a systemau parhaus. Mae hyn yn cynnwys rheoli'r pyrth sy'n cysylltu systemau OGCC â'r Rhyngrwyd er mwyn lleihau'r risgiau sy'n gysylltiedig â hacio, ymosodiadau o wrthod gwasanaeth, maleiswedd a mynediad heb awdurdod. Mae'r rheolaethau hyn yn berthnasol i draffig sy'n dod i mewn ac sy'n mynd allan.

9.2. Rheolir y gwaith o reoli cyfrifiaduron a rhwydweithiau drwy weithdrefnau tîm TG safonol sydd wedi'u dogfennu ac sydd wedi'u hawdurdodi gan yr ITM.

9.3. Rhaid i unrhyw fynediad i Rwydwaith OGCC gael ei ddiogelu â chyfrinair. Rhaid sefydlu systemau i wrthod cyfrineiriau nad ydyn nhw'n bodloni'r safonau cymhlethdod gofynnol.

9.4. **Cysylltu dyfeisiau â rhwydwaith OGCC**

Mae systemau a rhwydweithiau OGCC yn cadw cofnodion o ddyfeisiau sydd wedi'u cysylltu, yn ogystal â mynediad. Mae mynediad at systemau a rhwydweithiau Ombwdsmon Gwasanaethau Cyhoeddus Cymru wedi'i gyfyngu i ddyfeisiau OGCC ac unrhyw ddyfais arall (fel ffonau clyfar neu dabledi personol) sydd wedi'i hawdurdodi'n benodol gan OGCC. Mae pob defnydd yn amodol ar gyfyngiadau defnydd derbyniol fel y nodir yn y Polisi Safonau Ymddygiad Staff. Bydd meddalwedd rheoli dyfeisiau'n

cael ei ddefnyddio ar ddyfeisiau OGCC ac ar ddyfeisiau personol sy'n cael mynediad at systemau a rhwydweithiau OGCC (ac eithrio wifi i westeion).

9.5. Cof bach USB neu gyfryngau defnyddiwr tebyg

Dylid osgoi defnyddio cyfryngau cludadwy, megis dyfeisiau cof bach USB, CDs a DVDs i anfon gwybodaeth. Dylid anfon gwybodaeth yn electronig lle bynnag y bo modd. Mae rhagor o ganllawiau ar anfon gwybodaeth yn electronig i'w gweld yn y canllawiau mewnol Anfon gohebiaeth allanol.

Rhaid i unrhyw gyfryngau cludadwy a dderbynnir yn y post gael eu gwirio gan TG cyn iddo gael ei ddefnyddio mewn unrhyw ddyfais OGCC. Bydd angen iddo ymgymryd â sgan firws a gwirio nad yw'r cyfryngau cludadwy yn cynnwys unrhyw ffeiliau gweithredadwy na meddalwedd maleisus.

9.6. Dyfeisiau symudol (ee gliniaduron/tabledi/ffonau clyfar)

At ddibenion cyfarfodydd a pharhad busnes OGCC, gall yr Ombwdsmon roi ffonau clyfar a/neu gyfrifiaduron tabled sy'n eiddo i OGCC i staff awdurdodedig.

Rhaid i staff sydd wedi awdurdodi defnyddio dyfeisiau symudol yr Ombwdsmon gydymffurfio â gosodiadau penodol, gofynion diweddaru a defnyddio. Dylen nhw hefyd sicrhau diogelwch ffisegol y ddyfais symudol yn erbyn lladrad a/neu fynediad heb awdurdod at unrhyw ddata sydd yn y ddyfais symudol. Mae rhagor o fanylion am y mesurau i'w cymryd ar gael yn y canllawiau Sut mae gweithio'n ddiogel o gartref.

9.7. Rheoli newid

Cyn gosod a chychwyn, rhaid asesu risg pob system, rhaglen a rhwydwaith gwybodaeth newydd ar gyfer diogelwch. Bydd newidiadau i

systemau gwybodaeth, rhaglenni neu rwydweithiau yn cael eu hadolygu a'u cymeradwyo gan yr ITM.

Rhaid cynnal Asesiad o'r Effaith ar Ddiogelu Data er mwyn ystyried effaith newidiadau i unrhyw brosesu data personol. Mae'r Polisi Asesu Effaith ar Ddiogelu Data yn rhoi rhagor o wybodaeth am y broses hon.

10. Rheoli gwendidau

10.1. Mae enghreifftiau o wendidau systemau neu feddalwedd yn cynnwys meddalwedd sy'n gofyn am gywiro diffygion, neu efallai fod problemau ffurfweddu system hysbys. Gellir camfanteisio ar wendidau meddalwedd. Bydd y Tîm TG, gan weithio gyda'r Darparwr Cymorth TG, yn sicrhau bod y rhain yn cael eu nodi, eu hasesu a bod diweddariadau, cywiriadau ac atgyweiriadau'n cael eu rhoi ar waith yn brydlon.

10.2. Monitro diogelwch perimedr

Manylir ar hyn yn y Polisi Llywodraethu TG ac mae'n cynnwys y canlynol:

- Rhwystro e-bost drwy gynnwys a/neu atodiadau
- Dilysu wrth wirio negeseuon e-bost sy'n dod i mewn
- Muriau cadarn ar waith
- Gwahanu data ar systemau TG

10.3. Sganio gwendidau

Bydd OGCC yn sicrhau bod sganiau treiddio a gwendidau rheolaidd yn cael eu cynnal a'u hadrodd. Mae manylion yr amserlen a'r trefniant ar gyfer hyn i'w gweld yn y Polisi Llywodraethu TG.

10.4. Gwarchodaeth rhag meddalwedd maleisus

Rhaid i ddiogelwch rhag meddalwedd faleisus effeithiol fod ar waith ar gyfer holl systemau TG OGCC. Mae rhagor o fanylion am weithdrefnau

rheoli i ddiogelu ei hun rhag bygythiad meddalwedd maleisus ar gael yn y Polisi Llywodraethu TG. Yn ddiofyn, nid yw defnyddwyr yn gallu gosod meddalwedd ar eiddo'r sefydliad heb ganiatâd gan yr ITM.

10.5. **Systemau a meddalwedd cyfredol**

Bydd OGCC yn sicrhau bod yr holl gynhyrchion gwybodaeth yn cael eu trwyddedu a'u cymeradwyo'n briodol gan yr ITM. Ni fydd defnyddwyr yn gosod meddalwedd heb ganiatâd gan yr ITM. Rhaid i staff dderbyn a gosod diweddariadau ar OGCC, ac unrhyw ddyfeisiau eu hunain sydd wedi'u cysylltu â systemau neu rwydweithiau OGCC (ac eithrio wifi i westeion), yn rheolaidd ac yn brydlon.

10.6. **Cywiro a diweddaru**

Mae cywiriadau'n destun Polisi Rheoli Cywiriadau ar wahân yn unol â'r Polisi Llywodraethu TG i sicrhau bod meddalwedd a systemau'n cael eu cywiro'n llwyr ac yn amserol er mwyn cynnal diogelwch.

11. Diogelwch ffisegol ac amgylcheddol

11.1. Yn ogystal â diogelu mynediad at systemau gwybodaeth, mae Rhwydwaith TG OGCC hefyd yn cymryd camau i ddiogelu mynediad i'r adeilad, gan gynnwys mannau diogel.

11.2. Rhaid diogelu mynediad at gyfleusterau rhwydwaith a chyfathrebu, gan gynnwys ystafelloedd gweinydd a chanolfannau data yn ddigonol rhag difrod damweiniol (megis tân neu lifogydd), lladrad neu weithredoedd maleisus eraill. Dim ond staff awdurdodedig sydd ag angen busnes cyfiawn a chymeradwy fydd yn cael mynediad at fannau cyfyngedig sy'n cynnwys systemau gwybodaeth neu ddata wedi'i storio.

11.3. Mae drysau allanol i mewn i'r adeilad yn ddiogel ac mae modd cael mynediad atynt drwy ddefnyddio cod rhifol. Ni all aelodau'r cyhoedd gerdded i mewn i rannau cyffredin yr adeilad.

11.4. Mae pob drws i ardaloedd sy'n eiddo i OGCC yn cael ei ddiogelu gan glo ffisegol neu gan system cofnodi cardiau adnabod sy'n cael ei rheoli gan y Gwasanaethau Corfforaethol.

- Y Dderbynfa: Dim ond yn ystod oriau swyddfa y mae hwn ar agor i'r cyhoedd, a dim ond drwy ddrysau allanol y mae modd cael mynediad iddo. Mae mynediad o Dderbynfa OGCC i swyddfeydd OGCC hefyd yn cael ei reoli gan y system cofnodi cardiau.

- Swyddfa Gyffredinol: Caiff unrhyw aelod o staff awdurdodi mynediad i swyddfa cynllun agored OGCC yn ystod oriau swyddfa, ond rhaid mynd â'r ymwelydd at yr aelod perthnasol o staff y mae'n ymweld ag ef. Mae'r mynediad diofyn ar gyfer staff OGCC yn unig ynghyd â'r glanhawr swyddfa perthnasol.

- Ystafell Cyfathrebu TG: Y tîm TG sy'n rheoli'r awdurdodiad ar gyfer y mynediad hwn. Y mynediad diofyn yw 'dim mynediad' ar wahân i staff TG OGCC.

- Ystafell archif: Y Gwasanaethau Corfforaethol sy'n rheoli'r awdurdodiad ar gyfer y mynediad hwn. Y mynediad diofyn yw 'dim mynediad' ar wahân i'r Gwasanaeth Corfforaethol/Cymorth Gwaith Achos a Swyddogion Gwaith Achos y Tîm Cyngor ar Gwynion (CAT).

11.5. Er mwyn lleihau colled neu ddifrod i'r holl asedau, rhaid diogelu'r holl gyfarpar yn gorfforol rhag bygythiadau a pheryglon amgylcheddol ac yn amodol ar farciau diogelwch. Bydd yr holl gyfrifiaduron sydd wedi'u lleoli yn yr amgylchedd swyddfa agored (hynny yw heb eu storio mewn ystafell storio ddiogel â mynediad cyfyngedig) yn cael eu diogelu gan ddefnyddio cêbl cloi a diogelwch.

11.6. Rhaid i Dîm TG OGCC gadw rhestr o'r holl offer TG sydd wedi'i farcio i'w waredu ac sydd wedi storio gwybodaeth bersonol sydd ynddo, gan roi manylion y cwmni gwaredu a ddefnyddir. Mae'n rhaid cael cytundeb ysgrifenedig gydag OGCC a'r cwmni gwaredu sy'n nodi'r gofynion ar gyfer y gwarediad, a rhaid iddo gynnwys crybwyll y cwmni gwaredu fel y 'prosesydd data' o dan reolaeth OGCC fel y 'rheolydd data'. Rhaid hefyd cynnwys gofyniad i'r cwmni gwaredu ddinistrio gwybodaeth bersonol mewn modd diogel a rhoi tystysgrif ddinistrio i OGCC yn y cytundeb.

11.7. Rhaid i'r holl staff fod yn ymwybodol o'r angen i ddefnyddio mesurau diogelwch ffisegol megis:

- Cloi cypyrddau ffeilio a pheiriannau ffeilio ar yr ochr.
- Cloi sgriniau cyfrifiadur wrth gymryd seibiant a diffodd y cyfrifiadur a monitro pan na fydd y ddesg yn cael ei defnyddio am gryn amser (fel diwedd y dydd).
- Cau bleindiau swyddfa OGCC ar ddiwedd y dydd.
- Sicrhau bod gwybodaeth gyfrinachol OGCC yn cael ei chlirio o'r ddesg ar ddiwedd y dydd neu pan na fydd neb yn cadw llygad arni. Rhaid storio cofnodion meddygol gwreiddiol yn ddiogel yn y man diogel rhag tân y tu allan i oriau swyddfa arferol. Dylai staff drafod y trefniadau ar gyfer hyn gyda Chymorth Gwaith Achos neu'r Gwasanaethau Corfforaethol.
- Cael gwared ar wybodaeth gyfrinachol OGCC yn ddiogel pan nad oes ei hangen mwyach.
- Cadw cardiau mynediad, allweddi a chodau allweddol yn ddiogel bob amser.

Mae rhagor o ganllawiau i staff ar gael yn y canllawiau Sut mae gweithio'n ddiogel gartref.

12. Hunaniaeth a rheoli mynediad

12.1. Er mwyn sicrhau diogelwch gwybodaeth a systemau gwybodaeth OGCC, mae'n hanfodol bod cyfrifon mynediad defnyddwyr a hawliau mynediad yn cael eu rheoli'n effeithiol yn unol ag anghenion busnes. Y Tîm TG sy'n rheoli'r broses o gofrestru a dadgofrestru cyfrifon defnyddwyr drwy Gyfeiriadur Gweithredol.

12.2. Cyfyngir hawliau mynediad i'r isafswm sydd ei angen i alluogi'r defnyddiwr i gyflawni ei swydd.

12.3. **Dilysu Aml Ffactor**

Bydd lefelau mynediad at Systemau OGCC, gan gynnwys systemau sy'n cael eu lletya gan drydydd parti, yn cael eu rheoli a'u cyfyngu i'r defnyddwyr awdurdodedig hynny sydd ag angen busnes dilys. Mae rhagor o wybodaeth am hyn ar gael yn y Polisi Llywodraethu TG.

13. Rheoli Digwyddiadau Diogelwch Gwybodaeth

13.1. Mae OGCC wedi ymrwymo i leihau digwyddiadau diogelwch gwybodaeth a'u heffaith. Bydd achosion tybiedig yn cael eu hadrodd yn brydlon i'r IGM, ac i'r ITM os ydyn nhw'n ymwneud â TG. Ymchwilir i bob digwyddiad i sefydlu eu hachos a'u heffaith gyda'r bwriad o osgoi digwyddiadau tebyg ac i ganfod cyfleoedd i wella. Mae'r broses yn cael ei gosod yn y Polisi a Gweithdrefn Rheoli Digwyddiadau Diogelwch Gwybodaeth.

13.2. Mae'r IGM yn cadw cofnod canolog o ddigwyddiadau fel y gellir monitro cynnydd o ran rheoli ac ymchwilio i'r digwyddiad.

13.3. Rhaid i staff TG roi gwybod ar unwaith i'r COODOI ac IGM am unrhyw ddigwyddiadau seiberddiogelwch i'w cofnodi'n ganolog.

13.4. Mae'r adroddiadau Llywodraethu Gwybodaeth misol (a TG) i'r Tîm Rheoli yn rhoi crynodeb o'r digwyddiadau a adroddwyd a'r camau gweithredu dilynol. Mae adroddiadau chwarterol i'r Pwyllgor Archwilio a Sicrhau Risg hefyd yn cynnwys cyfeiriadau at reoli digwyddiadau.

13.5. Mae'r IGM, gyda chymorth y Grŵp Hyfforddiant IG, yn dadansoddi tueddiadau o ran digwyddiadau er mwyn cyfrannu at ragor o hyfforddiant diogelwch gwybodaeth ac anghenion cyfathrebu.

14. Diogelwch yn y gadwyn gyflenwi

14.1. Bydd contractau gyda chontractwyr allanol sy'n caniatáu mynediad i systemau gwybodaeth OGCC ar waith cyn y caniateir mynediad.

Bydd y contractau hyn yn sicrhau bod staff neu isgontractwyr y sefydliad allanol yn cydymffurfio â'r holl bolisïau diogelwch priodol.

14.2. Mae'n bwysig bod risgiau'r gadwyn gyflenwi yn cael eu harchwilio gyda'r cyflenwyr posib a bod mesurau rheoli diogelwch yn cael eu deall. Rhaid i bob contract gynnwys cyfeiriad at y gofyniad i'r cyflenwr roi gwybod ar unwaith i OGCC am unrhyw ddigwyddiadau neu risgiau diogelwch gwybodaeth.

15. Monitro ac Adrodd

15.1. Profir diogelwch pob system TG yn rheolaidd fel y nodir yn y Polisi Llywodraethu TG.

15.2. Bydd Archwiliadau Mewnol ar feysydd sy'n ymwneud â diogelwch gwybodaeth, gan gynnwys seiberddiogelwch, yn cael eu cynnwys yn y cynllun gwaith archwilio 3 blynedd mewnol.

15.3. Bydd yr ITM a/neu IGM yn rhoi gwybod i'r Tîm Rheoli am unrhyw faterion sy'n effeithio'n ddifrifol ar statws diogelwch gwybodaeth y sefydliad.

15.4. Bydd adroddiad blynyddol hefyd i'r tîm rheoli ac wedyn i'r Pwyllgor Archwilio a Sicrhau Risg a fydd yn cynnwys y canlynol:

- Mynediad TG: profion treiddio allanol.
- Mynediad TG: cydymffurfiad mewnol â'r polisi hwn.
- Monitro ymwelwyr.
- Profi cydymffurfiaeth wrth drosglwyddo gwybodaeth.
- Unrhyw ddigwyddiadau colli data a chamau gweithredu dilynol ers yr adroddiad diwethaf.

16. Adolygu

Bydd y Polisi Diogelwch Gwybodaeth yn cael ei gynnal a'i adolygu bob dwy flynedd a'i ddiweddaru gan yr ITM ac IGM.

17. Polisi / proses / canllawiau cysylltiedig

- Polisi Llywodraethu TG
- Polisi Safonau Ymddygiad Staff
- Anfon gohebiaeth allanol
- Gweithio gartref yn ddiogel
- Polisi a Gweithdrefn Rheoli Digwyddiadau Diogelwch Gwybodaeth.
- Polisi Rheoli Risg
- Polisi Parhad Busnes
- Cynllun Ymateb ac Adfer i Ddigwyddiad Seibr