Ombwdsmon
Ombudsman
Cymru • Wales

Polisi Diogelwch Gwybodaeth

Mae'r ddogfen hon hefyd ar gael yn y Gymraeg.
This document is also available in Welsh.

Cynnwys

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 anawdurdodedig neu anghyfreithlon a cholled, dinistr neu ddifrod damweiniol.

1.2 Mae gwerth i'r holl wybodaeth, gan gynnwys data personol, ac mae'n bwysig ein bod yn deall pa wybodaeth rydym ni'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. Rhaid i ni hefyd ystyried risgiau sefydliadol fel risgiau cyfreithiol, ariannol ac i enw da.

1.5 Mae'r polisi hwn yn elfen allweddol o fframwaith llywodraethu gwybodaeth cyffredinol yr OGCC 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, cymwysiadau, 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 a staff dros dro) ac unigolion neu sefydliadau sy'n cael eu contractio'n uniongyrchol gan OGCC.

3. Amcanion diogelwch gwybodaeth

3.1 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 byddwn 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 doriadau o'r fath.

4. Byrfoddau

EDCR	Cyfarwyddwr Gweithredol - Adnoddau Corfforaethol. At ddibenion llywodraethu gwybodaeth, cyfeirir ato hefyd fel Prif Swyddog Diogelwch Gwybodaeth (CISO).
HOITS	Pennaeth Gwasanaethau TG.
EDCL	Cyfarwyddwr Gweithredol - Gwaith Achos a Chyfreithiol (at ddibenion llywodraethu gwybodaeth, cyfeirir ato hefyd fel Uwch-berchennog Risg Gwybodaeth (SIRO).
IGM	Rheolwr Llywodraethu Gwybodaeth.

5. Rolau a chyfrifoldebau

5.1 Mae'r EDCR yn atebol i'r Ombwdsmon am lywodraethu gwybodaeth yn gyffredinol, gan gynnwys diogelwch gwybodaeth OGCC. Mae hyn yn cynnwys seiberddiogelwch a chadernid rhwydweithiau TG. Mae'r EDCR 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 Yr EDCL yw SIRO 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 HOITS a'r IGM, sy'n atebol i'r EDCL a'r EDCR.

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

5.5 Mae'r HOITS 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

Contractau cyflogaeth

7.1 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.

Proses staff newydd a staff sy'n gadael

7.2 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.

Newid rôl

7.3 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.

Hyfforddiant ac ymwybyddiaeth

7.4 Mae pawb yn gyfrifol am ddiogelwch gwybodaeth. Mae strategaeth hyfforddi ar lywodraethu gwybodaeth (IG) 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.

7.5 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.

Parhad busnes a chynlluniau Adfer ar ôl Trychineb

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

8.3 Rhaid i staff gadw deunydd sy'n gysylltiedig ag achosion yn y system rheoli achosion. Dylid cadw ffeiliau a chofnodion eraill i'r systemau perthnasol, neu i storfa ffeiliau rhwydwaith OGCC neu SharePoint sy'n cael ei derbyn ar hyn o bryd. Ni ddylai staff ddefnyddio storfa ffeiliau lleol ar fwrdd gwaith na disg caled eu cyfrifiaduron.

8.4 Mae manylion y trefniadau TG wrth gefn wedi'u cynnwys yn y Polisi Llywodraethu TG. Manylir ar y trefniadau wrth gefn yn y Polisi Llywodraethu TG, ac maent yn cynnwys:

- Trefniadau wrth gefn y cwmwl
- Trefniadau wrth gefn y systemau lletyol

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

8.6 Mae systemau wedi'u dylunio fel bod modd eu harchifo'n 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 wedi'i ddylunio, ei ffurfweddu, ei gynnal a'i reoli gan y tîm TG, ar y cyd â'r Darparwr Gwasanaeth TG a Reolir. 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 cysylltiadau rhwng systemau'r OGCC er mwyn lleihau'r risgiau sy'n gysylltiedig â hacio, ymosodiadau o wrthod gwasanaeth, maleiswedd a mynediad anawdurdodedig. 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 HOITS.

9.3 Rhaid diogelu unrhyw fynediad i Rwydwaith OGCC yn unol â'r safonau dilysu presennol. Rhaid sefydlu systemau i wrthod cyfrineiriau nad ydyn nhw'n bodloni'r safonau cymhlethdod gofynnol.

Cysylltu dyfeisiau â'r rhwydwaith TG

9.4 Mae systemau a rhwydweithiau TG OGCC yn cadw cofnodion o ddyfeisiau sydd wedi'u cysylltu, yn ogystal â mynediad. Mae mynediad at systemau a rhwydweithiau TG wedi'i gyfyngu i ddyfeisiau OGCC ac unrhyw ddyfais arall (fel dyfeisiau 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 a'r Polisi Defnyddio Dyfeisiau Personol. 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 Wi-Fi i westeion).

Dyfeisiau cof USB neu gyfryngau cludadwy tebyg

9.5 Dylid osgoi defnyddio cyfryngau cludadwy, fel dyfeisiau cof 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 ar gael yn y canllawiau mewnol ar anfon gohebiaeth allanol.

9.6 Rhaid i unrhyw gyfryngau cludadwy a dderbynnir yn y post gael eu gwirio cyn iddynt gael eu defnyddio mewn unrhyw ddyfais OGCC. Bydd y Tîm Cefnogi Gwaith Achos (CWS) yn cynnal sgan feirws ac yn gwirio nad yw'r cyfryngau cludadwy yn cynnwys unrhyw ffeiliau na meddalwedd maleisus y gellir eu gweithredu. Bydd y Tîm TG yn darparu cyngor a chefnogaeth i CWS.

Dyfeisiau symudol (e.e. gliniaduron / llechi / ffonau clyfar)

9.7 Mae'r rhan fwyaf o staff bellach yn defnyddio gliniadur OGCC, ac mae rhai staff awdurdodedig yn cael ffôn clyfar a/neu lechen OGCC.

9.8 Rhaid i staff gydymffurfio â'r gosodiadau penodol, a'r gofynion diweddaru a defnyddio ar gyfer y ddyfais symudol a roddir gan OGCC. Dylen nhw hefyd sicrhau diogelwch ffisegol y ddyfais symudol yn erbyn lladrad a/neu fynediad anawdurdodedig at unrhyw ddata sydd yn y ddyfais symudol. Mae rhagor o fanylion am y mesurau i'w cymryd ar gael yn y canllawiau ar Sut i weithio'n ddiogel.

Rheoli newid

9.9 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 HOITS.

9.10 Rhaid cynnal Asesiad o'r Effaith ar Ddiogelu Data er mwyn ystyried effaith newidiadau i unrhyw brosesu data personol. Mae'r Polisi Asesu Effaith Diogelu Data yn darparu 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.

Monitro diogelwch perimedr

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

- Rhwystro negeseuon ebost yn ôl cynnwys a/neu atodiadau
- Dilysu a gwirio negeseuon ebost sy'n dod i mewn
- Waliau tân ar waith
- Gwahanu data ar systemau TG
- Rheolaethau diogelwch ffisegol ar gyfer adeiladau

Sganio gwendidau

10.3 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.

Diogelu rhag maleiswedd

10.4 Rhaid i ddiogelwch rhag maleiswedd effeithiol fod ar waith ar gyfer holl systemau TG OGCC. Mae rhagor o fanylion am weithdrefnau rheoli i ddiogelu ei hun rhag bygythiad maleiswedd ar gael yn y Polisi Llywodraethu TG. Yn ddiofyn, nid yw defnyddwyr yn gallu gosod meddalwedd ar eiddo'r sefydliad heb ganiatâd gan yr HOITS.

Systemau a meddalwedd cyfredol

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

Cywiro a diweddaru

10.6 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. Logio a monitro

11.1 Bydd y tîm TG, gan weithio gyda'r Gwasanaeth TG a Reolir a Darparwyr Cymorth Seiberddiogelwch, yn cofnodi ac yn monitro digwyddiadau i benderfynu a yw ein systemau TG wedi cael eu peryglu ac, os felly, i ba raddau.

11.2 Bydd y Darparwyr yn darparu adroddiadau monitro a chofnodi digwyddiadau yn rheolaidd fel y cytunwyd gyda phob darparwr. Mae Tîm TG OGCC yn cael gwybod am ddigwyddiadau difrifol ar unwaith, a byddant yn cysylltu â darparwyr perthnasol i asesu ac ymateb i'r digwyddiad.

12. Diogelwch ffisegol ac amgylcheddol

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

12.2 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.

12.3 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.

12.4 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.

12.5 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'r dderbynfa ar agor i'r cyhoedd, a dim ond drwy ddrysau allanol y mae modd cael mynediad i'r dderbynfa. 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 awdurdodi mynediad i'r ystafell hon. Y mynediad diofyn yw 'dim mynediad' ar wahân i staff TG OGCC.
- **Ystafell bost:** Y Gwasanaethau Corfforaethol sy'n awdurdodi mynediad i'r ystafell hon. Mae'r mynediad diofyn ar gyfer staff OGCC.

12.6 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 diogelwch a chlo. Dylid storio gliniaduron yn ddiogel / dan glo ar ddiwedd y dydd.

12.7 Rhaid i dîm TG OGCC gynnal stocrestr o holl offer TG OGCC sydd wedi'i farcio i'w waredu, gan nodi 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 enw'r cwmni gwaredu fel y 'prosesydd data' o dan reolaeth OGCC fel y 'rheolydd data'. Yn ogystal, rhaid i'r cytundeb gynnwys gofyniad i'r cwmni gwaredu ddinistrio gwybodaeth bersonol mewn modd diogel a rhoi tystysgrif ddinistrio i OGCC.

12.8 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 gliniadur/cyfrifiadur wrth gymryd egwyl.
- Diffodd y ddyfais a monitro a symud gliniaduron pan mae'r ddesg yn mynd i fod yn wag am gryn amser (e.e. ar ddiwedd 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'r Swyddog Cymorth 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.

12.9 Mae rhagor o ganllawiau i staff ar gael yn y canllawiau ar Sut i weithio'n ddiogel.

13. Rheoli hunaniaeth a mynediad

13.1 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.

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

Dilysu Aml Ffactor

13.3 Bydd lefelau mynediad at Systemau OGCC, gan gynnwys systemau lletyol 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.

14. Rheoli Digwyddiadau Diogelwch Gwybodaeth

14.1 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 HOITS 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 manylion y broses i'w gweld yn y Polisi a Gweithdrefn Rheoli Digwyddiadau Diogelwch Gwybodaeth.

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

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

14.4 Mae'r adroddiadau IG a TG i'r Tîm Rheoli yn darparu crynodeb o'r digwyddiadau a adroddwyd a'r camau gweithredu dilynol. Mae adroddiadau chwarterol i'r Pwyllgor Archwilio a Sicrwydd Risg hefyd yn cynnwys cyfeiriadau at reoli digwyddiadau.

14.5 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.

15. Diogelwch yn y gadwyn gyflenwi

15.1 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.

15.2 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.

15.3 Rhaid i bob cyflenwr roi sicrwydd diogelwch ar ddechrau'r contract, a bydd hyn yn cael ei adolygu gyda nhw bob blwyddyn.

16. Monitro ac Adrodd

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

16.2 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.

16.3 Bydd yr HOITS a/neu IGM yn rhoi gwybod i'r Tîm Rheoli, ac wedyn i'r Pwyllgor Archwilio a Sicrwydd Risg, am y canlynol:

- Unrhyw faterion sy'n effeithio'n ddifrifol ar statws diogelwch gwybodaeth y sefydliad.
- Canlyniad unrhyw asesiadau cydymffurfio yn erbyn safonau diogelwch gwybodaeth.
- Canlyniad archwiliadau seiberddiogelwch a gynhaliwyd gan ddarparwr gwasanaeth seiberddiogelwch OGCC.

17. Adolygu

17.1 Bydd y Polisi Diogelwch Gwybodaeth yn cael ei gynnal a'i adolygu bob blwyddyn, a'i ddiweddaru gan yr HOITS ac IGM.

18. Polisïau / prosesau / canllawiau cysylltiedig

- Polisi Llywodraethu TG
- Polisi Safonau Ymddygiad Staff
- Anfon gohebiaeth allanol
- Gweithio'n ddiogel
- Polisi a Gweithdrefn Rheoli Digwyddiadau Diogelwch Gwybodaeth
- Polisi Rheoli Risg
- Cynllun Parhad Busnes
- Gweithdrefnau Ymateb i Ddigwyddiadau