Cyfeirnod: Fersiwn 3.4
Dyddiad cyhoeddi: Mawrth 2020
Cyswllt allweddol: [redacted]

Polisi Diogelwch Gwybodaeth

Cynnwys

Hanes diwygio

Fersiwn	Crynodeb o'r newidiadau	Dyddiad
F1.0	Cwblhau'r fersiwn gyntaf.	Chwefror 2006
F1.1	Newid Swyddog Diogelwch Gwybodaeth, wedi diwygio paragraff 29 fel bod cyswllt â rhwydwaith band eang cartref yn cael ei ganiatáu.	Hydref 2007
F2.0	Diwygiad mawr gan gynnwys canllawiau manylach ar 'ofalu am offer' a 'chael data busnes gan gyrff a archwilir'.	Hydref 2008
F2.1	Newid yn adlewyrchu bod offer Swyddfa Archwilio Cymru e.e. gliniaduron, cofau bach yn gallu cael eu gadael heb neb i ofalu amdanynt mewn cerbydau am hyd at bedair awr os ydynt wedi'u cuddio a'u cloi yn y gist, neu rywle cyfatebol.	Mai 2009
F2.2	Diwygiad i'r adran ar Fonitro a Gorfodi Diogelwch, gan egluro y bydd monitro rheolaidd yn digwydd. Bydd y monitro'n gwirio cydymffurfiaeth staff â'r gyfraith a'r Polisi Diogelwch Gwybodaeth hwn. Mynediad at wefannau rhwydweithio cymdeithasol a gwefannau e-bost allanol wedi'i wahardd.	Gorffennaf 2010
F2.3	Cynnwys deunydd i ddarparu eglurhad o ddefnydd annerbyniol o gyfleusterau prosesu gwybodaeth. Cynnwys atodiad 3 newydd sy'n nodi polisi monitro rheolaidd manwl.	Medi 2011
F3.0	Diwygiad mawr – Mae'r Polisi Diogelwch Gwybodaeth bellach yn canolbwyntio ar ofynion ymarferol. Mae egwyddorion prosesu gwybodaeth lefel uwch, ynghyd â rolau a chyfrifoldebau, bellach i'w cael yn y Polisi Llywodraethu Gwybodaeth ar wahân.	Ebrill 2015

F3.1	Cynnwys paragraff newydd i amlinellu gweithdrefnau tanseilio diogelwch data er mwyn cydymffurfio â'r Rheoliad Cyffredinol ar Ddiogelu Data.	Awst 2017
F3.2	Newid i hysbysu sut y gellir trosglwyddo data gan ddefnyddio ffeiliau Microsoft â threfniadau cryf i ddiogelu â chyfrinair.	Chwefror 2018
F3.3	Newidiadau i ddiffinio categorïau data'n fwy eglur.	Mai 2018
F3.4	Egluro'r trefniadau ar gyfer defnyddio a diogelu dyfeisiau personol	Mawrth 2020

Crynodeb

1 Mae'r gofynion yn y polisi hwn yn berthnasol i'r holl gyflogeion, aelodau anweithredol a chontractwyr, boed yn cael eu cyflogi trwy asiantaeth, neu'n uniongyrchol. Er byrder, yn y ddogfen hon mae'r diffiniad o 'staff' yn cynnwys yr holl gategorïau hyn o bobl.

2 Mae'r polisi hwn yn disgrifio'r camau ymarferol y mae'n rhaid i staff eu cymryd er mwyn cadw gwybodaeth y sefydliad yn ddiogel.

3 Er bod ffocws ymarferol i'r polisi hwn, dylid ei ddarllen ar y cyd â'r Polisi Llywodraethu Gwybodaeth, dogfen lefel uwch sy'n cwmpasu egwyddorion prosesu gwybodaeth a'r rolau a chyfrifoldebau cysylltiedig.

4 Mae'n ofynnol i'r holl staff ymgyfarwyddo â'r Polisi Diogelwch Gwybodaeth hwn, a chadarnhau mewn datganiad blynyddol wrth Adran y Gyfraith a Moeseg (neu Ysgrifennydd y Bwrdd yn achos aelodau'r bwrdd) eu bod wedi darllen a deall y cynnwys.

5 Mae'r ddogfen hon yn cynnwys polisi swyddogol y sefydliad. Dangosir yr hanes diwygio ar y clawr.

System Rheoli Diogelwch Gwybodaeth

6 Mae Swyddfa Archwilio Cymru wedi mabwysiadu'r Safon Ryngwladol ar gyfer Systemau Rheoli Diogelwch Gwybodaeth (ISO 27001) y mae ei hegwyddorion yn cynnwys:

7 mynd ati mewn modd systematig i archwilio ac asesu'r risgiau i ddiogelwch gwybodaeth Swyddfa Archwilio Cymru, gan ystyried y bygythiadau, bregusrwydd ac effeithiau;

8 dylunio a gweithredu casgliad cydlynus a chynhwysfawr o reolaethau diogelwch gwybodaeth a/neu ffyrdd eraill o drin risgiau i sicrhau bod risgiau'n cael eu lleihau i lefel dderbyniol; a

9 mabwysiadu proses reoli drosfwaol i sicrhau bod y rheolaethau diogelwch gwybodaeth yn parhau i ddiwallu anghenion diogelwch gwybodaeth y sefydliad yn barhaus.

Cyfrifoldebau staff

Enwau defnyddwyr a chyfrineiriau

10 Bydd pob aelod o staff yn cael cyfuniad o enw defnyddiwr a chyfrinair i'w ddefnyddio gyda systemau Swyddfa Archwilio Cymru, er enghraifft wrth fewngofnodi ar liniadur, neu adfer slip cyflog misol. Rhaid peidio â rhannu cyfrineiriau o'r fath gyda chydweithwyr. Cysylltwch â'r tîm TG os nad ydych yn gallu cael mynediad at y systemau neu'r adnoddau y mae eu hangen arnoch

11 Dylid dewis cyfrineiriau cofiadwy, ac ni ddylent byth gael eu hysgrifennu i lawr.

Cysylltu offer personol neu offer nad yw'n perthyn i Swyddfa Archwilio Cymru

12 Gall ffonau clyfar neu gyfrifiaduron personol neu rai sy'n perthyn i ymwelwyr gael eu cysylltu â'r Rhyngrwyd trwy WiFi ymwelwyr Swyddfa Archwilio Cymru – chwiliwch am 'guest WiFi' ar yr Hwb i gael y manylion. Ni ddylai offer nad yw'n perthyn i Swyddfa Archwilio Cymru gael ei gysylltu mewn unrhyw ffordd arall – er enghraifft trwy gebl rhwydwaith.

Gofalu am offer a gwybodaeth

13 Er bod data ar liniaduron a ffonau clyfar Swyddfa Archwilio Cymru wedi'i ddiogelu trwy ei amgryptio, rhaid i staff gymryd camau rhesymol i ofalu am offer Swyddfa Archwilio Cymru. Rhaid i staff gymryd pob cam rhesymol i ofalu am wybodaeth Swyddfa Archwilio Cymru a gaiff ei phrosesu ar ddyfeisiau personol neu a ddelir ar bapur hefyd. Bydd achos o ddwyn neu golli offer neu wybodaeth Swyddfa Archwilio Cymru oherwydd methiant i gymryd gofal rhesymol yn cael ei drin fel mater difrifol.

14 Rhaid i staff beidio â gadael offer na gwybodaeth Swyddfa Archwilio Cymru heb neb i ofalu amdanynt lle mae risg y gallent gael eu dwyn – er enghraifft, ar agor (sgrîn wedi'i datgloi) ar y bwrdd yn ystod siwrnai ar drên, neu mewn ystafell gyfarfod mewn gwesty yn ystod amser cinio.

15 Gellir gadael offer a gwybodaeth Swyddfa Archwilio Cymru heb neb i ofalu amdanynt mewn car am hyd at 4 awr, ar yr amod eu bod yn cael eu cuddio o'r golwg a bod y car wedi'i gloi – ond byth dros nos.

16 Gall staff adael offer a gwybodaeth Swyddfa Archwilio Cymru heb unrhyw un i ofalu amdanynt ar safleoedd swyddfeydd lle ceir 'diogelwch terfyn allanol' rhesymol h.y. mesurau i atal pobl anawdurdodedig rhag mynd i mewn i'r swyddfa, neu gartref.

17 Rhaid i holl offer a gwybodaeth Swyddfa Archwilio Cymru gael eu dychwelyd trwy'r rheolwr llinell pan fo cyflogaeth yn dod i ben, neu drwy'r Gwasanaethau Busnes yn achos aelodau'r Bwrdd.

Cael a chyfleu gwybodaeth

18 Mae Swyddfa Archwilio Cymru'n rhannu gwybodaeth yn dri chategori. Mae gwahanol ragofalon ar gyfer trin gwybodaeth yn berthnasol, gan ddibynnu ar y categori:

a. **Data hynod sensitif – gwybodaeth sydd, pe bai'n cael ei datgelu'n amhriodol, â'r potensial i achosi trallod neu niwed difrifol i unigolion neu niwed difrifol i enw da neu fuddiannau Archwilydd Cyffredinol Cymru, Swyddfa Archwilio Cymru neu bartïon eraill megis cyrff a archwilir, Gweinidogion Cymru a Chynulliad Cenedlaethol Cymru.** Bydd hyn yn cynnwys gwybodaeth am drethdalwyr, fel a ddiffinnir gan Ddeddf Casglu a Rheoli Trethi (Cymru) 2016, ac unrhyw ddata personol arwyddocaol, er enghraifft ffeil cyflogres corff a archwilir sy'n cynnwys enwau, cyfeiriadau a manylion banc a ddefnyddir gyda thechnegau archwilio gyda chymorth cyfrifiadur (CAATs), neu wybodaeth a gyflwynwyd gan Swyddfa Archwilio Cymru i'r Adran Gwaith a Phensiynau sy'n cynnwys manylion cyfraniadau pensiwn cyflogeion. Ni ddylai gwybodaeth o'r fath ond cael ei throsglwyddo a'i phrosesu:

   i. ar ôl adolygiad gan Swyddog Diogelu Data (SDD) Swyddfa Archwilio Cymru a fydd yn cynghori ynghylch y mesurau diogelwch sy'n ofynnol a, lle y bo'n briodol, yn cynnal cyswllt â'r Swyddog Diogelu Data yn y corff a archwilir;

   ii. gan ddefnyddio dull amgryptio diogel, gorau oll os taw neges e-bost wedi'i hamgryptio ydyw (gweler yr hwb) neu amgryptio ar y we[1];

[1] Os nad yw neges e-bost wedi'i hamgryptio neu ddull amgryptio seiliedig ar y we yn ymarferol, gallwch drosglwyddo gwybodaeth o law i law i gysylltiadau a enwir trwy drefniant ymlaen llaw gan ddefnyddio cof bach wedi'i amgryptio. Fel arall, gallwch ddefnyddio ffeiliau Microsoft Office ynghyd â threfniant cryf i ddiogelu â chyfrinair gyda'r cyfrinair yn cael ei gyfleu i'r derbynnydd ar wahân a

iii. yn unol â gweithdrefnau penodol a awdurdodwyd ar gyfer y broses fusnes dan sylw. Er enghraifft, mae polisi penodol ar gyfer data technegau archwilio gyda chymorth cyfrifiadur, ni ellir ond ei storio ar beiriant wedi'i amgryptio sy'n annibynnol ac nad yw'n gadael safle Swyddfa Archwilio Cymru, a rhaid ei ddileu cyn gynted ag y mae'r gwaith archwilio wedi'i gwblhau.

b. **Data sensitif – gwybodaeth sydd â'r potensial i gael effaith negyddol ar unigolion neu fuddiannau neu enw da Archwilydd Cyffredinol Cymru, Swyddfa Archwilio Cymru neu bartïon eraill megis cyrff a archwilir, Gweinidogion Cymru a Chynulliad Cenedlaethol Cymru.** Mae enghreifftiau'n cynnwys:

   i. adroddiadau cyn cyhoeddi y mae'r wasg yn dangos diddordeb ynddynt, neu sydd ag effaith sylweddol ar unigolion, sy'n ymwneud â chamwedd, neu sy'n sensitif yn wleidyddol; a

   ii. adroddiadau neu lythyrau a ddrafftiwyd mewn ymateb i gŵyn

   iii. negeseuon e-bost neu ddogfennau sy'n cynnwys data personol.

   Gall data o'r math yma gael ei storio ar liniadur o eiddo Swyddfa Archwilio Cymru am gyhyd ag y gweithir arno ond rhaid ei ddileu o'r gliniadur unwaith y mae'r gwaith wedi'i gwblhau.

   Rhaid i staff ddefnyddio dull diogel o gyfnewid data o'r math yma, er enghraifft, neges e-bost wedi'i hamgryptio, os yw'r derbynnydd bwriadedig yn gallu defnyddio hyn.

c. **Data arall –** data nad yw wedi'i gwmpasu gan y categorïau uchod yw hyn ac mae'n cynnwys, er enghraifft, gwybodaeth weithio gyffredinol ar gyfer archwiliad a chofnodion cyfarfodydd.

   Gall y math yma o ddata gael ei storio ar liniaduron fel y bo angen. Gellir defnyddio e-bost rhyngrwyd, arferol i'w gael neu ei gyfnewid.

19 Rhaid i staff eu gwneud eu hunain yn ymwybodol o unrhyw ofynion neu bolisïau penodol sydd gan gorff a archwilir a'u dilyn, er enghraifft ar gyfer dogfennau y dylid rhoi marc gwarchod arnynt. Fodd bynnag, os yw gofynion corff a archwilir i'w gweld yn rhy feichus fel eu bod yn atal mynediad at ddibenion archwilio, dylai staff godi'r mater gydag Adran y Gyfraith a Moeseg.

Cofau bach (a elwir hefyd yn gofbinnau neu yriannau USB)

thrwy ddull gwahanol. Gall hyn fod yn ddefnyddiol ar gyfer cyfleu gwybodaeth hynod sensitif, megis adroddiadau disgyblu, yn fewnol. Fodd bynnag, bydd ffeiliau a ddiogelwyd â chyfrinair sy'n dod i mewn i Swyddfa Archwilio Cymru yn cael eu rhoi dan gwarantîn, felly bydd angen i chi ofyn i'r adran TG eu rhyddhau.

20 Ni ddylai cofau bach heb eu hamgryptio, nad oes angen cyfrinair ar eu cyfer, byth gael eu defnyddio gyda data Swyddfa Archwilio Cymru.

21 Dylai staff osgoi defnyddio cofau bach wedi'u hamgryptio hefyd. Fodd bynnag, gellir defnyddio cof bach o'r fath os mai dyma yw'r unig opsiwn diogel sy'n rhesymol ymarferol; er enghraifft, os nad yw defnyddio neges e-bost wedi'i hamgryptio neu drosglwyddo ffeil yn ddiogel trwy borth ar y we (e.e. Egress) yn ymarferol.

Defnyddio "dyfeisiau staff eu hunain" megis ffonau clyfar personol ar gyfer gwaith Swyddfa Archwilio Cymru

22 Mae Swyddfa Archwilio Cymru'n deall ei bod yn gyfleus ac yn effeithiol i'r sefydliad (yn ogystal â staff) bod staff yn defnyddio'u dyfeisiau eu hunain ar gyfer gwaith Swyddfa Archwilio Cymru. Fodd bynnag, Swyddfa Archwilio Cymru sy'n dal i fod yn gyfrifol am brosesu ei data, hyd yn oed os gwneir hynny ar ddyfeisiau o'r fath. Felly, mae prosesu data Swyddfa Archwilio Cymru, megis defnyddio ap Outlook Swyddfa Archwilio Cymru ar gyfer e-bost, ar ddyfeisiau staff eu hunain yn ddarostyngedig i ofynion y Polisi Llywodraethu Gwybodaeth a'r adrannau "Cyfrifoldebau staff" a "Hysbysu ynghylch digwyddiadau diogelwch" yn y polisi hwn. Rhaid i staff wneud pob ymdrech rhesymol i sicrhau bod gwybodaeth o eiddo Swyddfa Archwilio Cymru y maent yn ei phrosesu ar eu dyfeisiau eu hunain yn ddiogel. I wneud hyn, rhaid i staff gyfeirio at ***Bolisi a Chanllawiau Dod â'ch Dyfais Eich Hun*** Swyddfa Archwilio Cymru ar yr Hwb i wirio a yw eu defnydd o'u dyfais yn ddigon diogel ac, os oes angen, cael cyngor gan y tîm TG.

Creu copïau wrth gefn o ddata

23 Mae copïau wrth gefn o wybodaeth a ddelir ar systemau Swyddfa Archwilio Cymru, er enghraifft Insight neu Sharepoint ar-lein, yn cael eu creu'n awtomatig. Nid oes angen i staff gymryd camau penodol i greu copïau wrth gefn.

24 Rhaid i staff gymryd camau i greu copïau wrth gefn o waith, lle mae'r unig gopi cyfoes ar liniadur unigolyn. Er enghraifft, ar ddiwedd diwrnod pan fo aelod o staff wedi bod yn diweddaru adroddiad penodol, dylai'r fersiwn ddiweddaraf gael ei chadw i Sharepoint neu'r system Insight. Bydd hyn yn gochel rhag colli gwybodaeth pe bai'r gliniadur yn methu, sy'n gallu digwydd weithiau heb rybudd.

25 Sylwer, yn wahanol i'r prif flwch negeseuon e-bost, **nad** oes copïau wrth gefn o 'ffolderi personol' yn Outlook, a adwaenir hefyd fel ffeiliau PST, yn cael eu creu'n awtomatig. Dylai staff fynd ati eu hunain i greu copïau wrth gefn o'r rhain os ydynt yn cael eu defnyddio.

Defnydd derbyniol

26 Rhaid i staff beidio â defnyddio offer Swyddfa Archwilio Cymru mewn unrhyw ffordd a allai niweidio enw da'r sefydliad. Er enghraifft, ni ddylai staff anfon, storio na chael mynediad yn fwriadol at ddeunydd sydd:

- yn anllad neu'n bornograffig;
- yn debygol o achosi tramgwydd cyffredinol;
- yn faleisus, yn ddifrïol neu'n ddifenwol o ran ei natur;
- yn hiliol, yn rhywiaethol neu'n gyfystyr fel arall â gwahaniaethu anghyfreithlon o ran nodweddion gwarchodedig a ddiffinnir gan Ddeddf Cydraddoldeb 2010 (h.y. o ran oedran, nam (anabledd), ailbennu rhywedd, priodas a phartneriaeth sifil, beichiogrwydd a mamolaeth, hil, crefydd neu gred, rhyw (rhywedd) a chyfeiriadedd rhywiol); neu
- yn gyfystyr ag aflonyddu.

27 Gall staff ddefnyddio offer Swyddfa Archwilio Cymru at ddibenion personol, er enghraifft bancio ar-lein, siopa neu ddarllen y newyddion, ar yr amod bod yr amser a dreulir yn gwneud hynny'n gyfnod gweddol fyr o 'egwyl o'r gwaith'. Ni ddylai staff ddefnyddio gwe-bost personol ar liniaduron Swyddfa Archwilio Cymru.

28 Lle mae defnydd personol o offer Swyddfa Archwilio Cymru'n ysgwyddo cost, er enghraifft galwadau personol ar ffonau symudol neu ffonau desg, rhaid cyfyngu hyn i £5 yr aelod o staff y mis neu fel arall rhaid ad-dalu'r gost.

29 Gall staff ddefnyddio'r cyfryngau cymdeithasol, yn amodol ar Bolisi Cyfryngau Cymdeithasol y sefydliad, sydd ar yr Hwb. Ar y cyfan, dylai staff fod yn ymwybodol bod y rheolau a'r egwyddorion ymddygiad y mae'n rhaid eu dilyn yn y byd go iawn yn berthnasol yn y byd ar-lein hefyd.

30 Rhaid i staff eu gwneud eu hunain yn ymwybodol o unrhyw ofynion neu bolisïau penodol sydd gan gorff a archwilir a dilyn y rheiny wrth ddefnyddio'i gyfrifiaduron neu ei systemau.

Monitro diogelwch

31 Mae Swyddfa Archwilio Cymru'n defnyddio ystod o dechnegau monitro i sicrhau bod gwybodaeth a systemau'n cael eu diogelu'n briodol, a bod staff yn cydymffurfio â pholisïau Swyddfa Archwilio Cymru a'r gyfraith.

32 Bydd Swyddfa Archwilio Cymru'n sicrhau bod trefniadau monitro'n rhesymol ac yn gymesur â'r risgiau.

33 Rhaid i staff dderbyn y gall unrhyw ddefnydd o offer Swyddfa Archwilio Cymru, boed ar gyfer busnes neu at ddibenion personol, gael ei recordio, y gellir craffu arno neu ymchwilio iddo trwy'r dulliau awtomatig neu'r dulliau â llaw hyn.

Hysbysu ynghylch digwyddiadau diogelwch

34 Rhaid i staff hysbysu'r ddesg gymorth TG ynghylch digwyddiadau diogelwch. Gallai'r rhain gynnwys achosion lle, e.e. mae staff corff a archwilir wedi anfon gwybodaeth bersonol a sensitif trwy e-bost rhyngrwyd arferol, neu lle mae gliniadur wedi cael ei ddwyn. Dylai hysbysu'n ddiymdroi ei gwneud yn bosibl cymryd camau cywirol a helpu Swyddfa Archwilio Cymru a chyrff eraill i ddysgu a gwneud unrhyw newidiadau angenrheidiol i osgoi digwyddiad arall tebyg.

35 Bydd y ddesg gymorth TG yn hysbysu'r Swyddog Diogelwch Gwybodaeth a Phennaeth y Gyfraith a Moeseg ynghylch unrhyw ddigwyddiad, a bydd y swyddog hwnnw'n cynnal cyswllt ynghylch ymdrin ag ef. Bydd Adran y Gyfraith a Moeseg yn asesu ac yn cofnodi'r digwyddiad ac yn ystyried camau nesaf yn unol â rhestr wirio tanseilio diogelwch data, gan gynnwys unrhyw gyfathrebu sy'n ofynnol gyda rhanddeiliaid mewnol ac allanol a Swyddfa'r Comisiynydd Gwybodaeth.

Cael help

36 Os oes arnoch angen cyngor ynghylch unrhyw beth yn y polisi hwn, neu unrhyw agwedd ymarferol ar weithio gyda gwybodaeth ar offer Swyddfa Archwilio Cymru, cysylltwch â'r tîm TG ar 02920 320690 neu drwy Skype neu'r e-bost yn "Cymorth TG/IT Support".