Policy and procedure

WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Cyfeirnod: Fersiwn 3.1
Dyddiad cyhoeddi: Chwefror 2018
Person cyswllt allweddol: Matthew Jubb

Polisi Diogelu Gwybodaeth

Cynnwys

Hanes yr adolygiadau

Fersiwn	Crynodeb o'r newidiadau	Dyddiad
V1.0	Cwblhau'r fersiwn gyntaf.	Chwefror 2006
V1.1	Newid y Swyddog Diogelu Gwybodaeth, addasu paragraff 29 fel y caniateir cysylltiad â rhwydwaith band eang cartref.	Hydref 2007
V2.0	Adolygiad mawr gan gynnwys canllawiau mwy manwl ar 'ofalu am gyfarpar' a 'chael data busnes gan gyrff a archwilir'.	Hydref 2008
V2.1	Newid sy'n nodi y gellir gadael cyfarpar Swyddfa Archwilio Cymru, fel gliniaduron a chof bach, heb eu monitro mewn cerbydau hyd at bedair awr, ar yr amod eu bod yn guddiedig ac wedi eu cloi yn y gist neu gyfatebol.	Mai 2009
V2.2	Adolygiad i adran Monitro a Gorfodi Diogelwch, sy'n esbonio y cynhelir gweithredoedd monitro yn rheolaidd. Bydd hyn yn cynnwys gwirio a yw staff yn cydymffurfio â'r gyfraith ac â'r Polisi Diogelwch Gwybodaeth hwn. Gwahardd mynediad at rwydweithiau cymdeithasol a gwefannau e-bost allanol.	Gorffennaf 2010
V2.3	Cynnwys deunyddiau i egluro ystyr defnydd annerbyniol o gyfleusterau prosesu gwybodaeth. Cynnwys atodiad 3 newydd, sy'n nodi polisi monitro rheolaidd manwl.	Medi 2011
V3.0	Adolygiad mawr – mae'r Polisi Diogelu Gwybodaeth yn canolbwyntio erbyn hyn ar ofynion ymarferol. Mae egwyddorion prosesu gwybodaeth lefel uwch, ynghyd â swyddogaethau a chyfrifoldebau, wedi'u cynnwys yn awr mewn Polisi Llywodraethu Gwybodaeth ar wahân.	Ebrill 2015
V3.1	Cynnwys paragraff newydd i amlinellu gweithdrefnau i'w dilyn mewn achosion o fynediad diawdurdod at ddata, er mwyn cydymffurfio â'r Rheoliad Diogelu Data Cyffredinol.	Awst 2017
V3.2	Newid i roi gwybod sut y gellir trosglwyddo data gan ddefnyddio ffeiliau Microsoft wedi'u diogelu â chyfrinair cryf.	

Crynodeb

1 Mae'r gofynion yn y polisi hwn yn berthnasol i'r holl aelodau staff, aelodau nad ydyn yn weithredol a chontractwyr, pa un a ydynt wedi eu cyflogi drwy asiantaeth neu'n uniongyrchol. Er mwyn bod yn gryno, mae'r diffiniad o staff yn y ddogfen hon yn cynnwys yr holl gategorïau o bobl a nodwyd uchod.

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

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

4 Mae'n ofynnol i bob aelod o staff ymgyfarwyddo â'r Polisi Diogelu Gwybodaeth hwn, ac i gadarnhau ei fod wedi'i ddarllen ac wedi deall y cynnwys.

5 Mae'r ddogfen hon yn cynnwys polisi swyddogol y sefydliad. Mae hanes yr adolygiadau ar gael ar y daflen eglurhaol.

System Rheoli Diogelwch Gwybodaeth

6 Mae Swyddfa Archwilio Cymru wedi mabwysiadu'r Safon Ryngwladol ar gyfer Systemau Rheoli Diogelwch Gwybodaeth (ISO 27001) sy'n cynnwys yr egwyddorion canlynol:

a) archwilio ac asesu'n systematig y risgiau a all fod i ddiogelwch gwybodaeth Swyddfa Archwilio Cymru, gan ystyried y bygythiadau, y gwendidau a'r effeithiau;

b) cynllunio a gweithredu cyfres o reolaethau diogelu gwybodaeth, a/neu ffurfiau eraill o ymdrin â risgiau, sy'n gydlynol a chynhwysfawr er mwyn sicrhau bod y risgiau wedi eu lleihau i lefel dderbyniol; ac

c) mabwysiadu proses reoli drosfwaol i sicrhau bod y rheolaethau diogelu gwybodaeth yn parhau i ddiwallu anghenion diogelu gwybodaeth y sefydliad yn barhaus.

Cyfrifoldebau'r staff

Enwau defnyddwyr a chyfrineiriau

7 Darperir enw defnyddiwr a chyfrinair i bob aelod o staff ar gyfer defnyddio systemau Swyddfa Archwilio Cymru, er enghraifft, wrth fewngofnodi ar liniadur, neu chwilio am slipiau cyflog. Ni chaniateir rhannu cyfrineiriau o'r fath â chydweithwyr. Cysylltwch â'r tîm TG os nad ydych yn gallu mynd i mewn i'r systemau neu'r adnoddau sydd eu hangen arnoch chi.

8 Dylid newid y cyfrinair i rywbeth y gellir ei gofio, ac ni ddylid byth ei gofnodi ar bapur.

Cysylltu cyfarpar personol a chyfarpar nad yw'n perthyn i Swyddfa Archwilio Cymru

9 Ceir cysylltu ffonau clyfar neu gyfrifiaduron personol neu rai sy'n perthyn i ymwelwyr â'r Rhyngrwyd drwy'r WiFi i westeion sydd gan Swyddfa Archwilio Cymru – chwiliwch am 'guest WiFi' ar yr Hub i gael rhagor o fanylion. Ni chaniateir cysylltu cyfarpar nad yw'n perthyn i Swyddfa Archwilio Cymru mewn unrhyw ffordd arall – er enghraifft drwy gebl rhwydwaith.

Gofalu am gyfarpar

10 Er bod data ar liniaduron a ffonau clyfar Swyddfa Archwilio Cymru wedi'i ddiogelu drwy amgryptio, mae'n rhaid i aelodau staff ofalu'n rhesymol am gyfarpar Swyddfa Archwilio Cymru. Byddwn yn trin lladrad neu golli cyfarpar fel mater difrifol, os yw o ganlyniad i fethu â chymryd gofal rhesymol.

11 Mae'n rhaid i aelodau staff beidio â gadael cyfarpar Swyddfa Archwilio Cymru heb oruchwyliaeth lle y ceir risg o ladrad – er enghraifft, ar agor (h.y. sgrin heb ei gloi) ar y bwrdd ar daith drên, neu mewn ystafell gyfarfod nad yw wedi'i chloi mewn gwesty yn ystod amser cinio.

12 Ceir gadael cyfarpar Swyddfa Archwilio Cymru heb oruchwyliaeth mewn car am hyd at 4 awr, ar yr amod ei fod wedi'i guddio a bod y car wedi'i gloi – ond byth dros nos.

13 Caiff aelodau staff adael cyfarpar Swyddfa Archwilio Cymru heb oruchwyliaeth mewn swyddfeydd gyda diogelwch ffiniau allanol rhesymol, h.y. mesurau i atal pobl nad ydynt wedi eu hawdurdodi rhag mynd i mewn i'r swyddfa, neu gartref.

14 Mae'n rhaid dychwelyd yr holl gyfarpar pan ddaw'r gyflogaeth i ben, a hynny drwy law'r rheolwr llinell.

Cael a throsglwyddo gwybodaeth

15 Mae Swyddfa Archwilio Cymru yn dosbarthu gwybodaeth i dri chategori. Mae gwahanol ragofalon trin a thrafod yn gymwys, gan ddibynnu ar y categori:

a) **Data sensitif iawn –** bydd hyn fel arfer yn cynnwys data personol arwyddocaol, er enghraifft, ffeil gyflogres corff a archwilir, sy'n cynnwys enwau, cyfeiriadau a manylion banc a ddefnyddir drwy dechnegau â chymorth cyfrifiadurol (CAAT), neu wybodaeth a gyflwynir gan Swyddfa Archwilio Cymru i Adran Gwaith a Phensiynau sy'n cynnwys manylion cyfraniadau pensiwn cyflogeion. Ni ddylid trosglwyddo a phrosesu gwybodaeth o'r fath oni bai:

- bod trefniadau blaenorol wedi'u gwneud â'r Pwynt Cyswllt Unigol yn Swyddfa Archwilio Cymru a'r Pwynt Cyswllt Unigol yn y corff a archwilir;
- y caiff ei wneud drwy ddull diogel wedi'i amgryptio, megis amgryptio ar y we, wyneb i wyneb rhwng unigolion cyswllt a drefnir ymlaen llaw drwy gof bach wedi'i amgryptio, neu drwy ddefnyddio diogelwch cyfrinair cryf ar ffeiliau Microsoft Office gan anfon y cyfrinair at y derbynnydd ar wahân a thrwy ddull gwahanol; ac
- y gwneid hynny yn unol â gweithdrefnau penodol wedi eu hawdurdodi ar gyfer y broses fusnes dan sylw. Er enghraifft, mae data CAAT yn ddarostyngedig i bolisi arbennig. Ni chaniateir ei storio ac eithrio ar

beiriant ar wahân wedi ei amgryptio, ni chaniateir iddo adael adeilad Swyddfa Archwilio Cymru, ac mae'n rhaid ei ddileu cyn gynted ag y daw'r gwaith archwilio i ben.

b) **Data sensitif –** mae enghreifftiau yn cynnwys:

– adroddiadau cyn cyhoeddi gwybodaeth, pan fo'r wasg â diddordeb ynddynt, neu pan fo effaith sylweddol ar unigolion, yn ymwneud â thorri rheolau, neu'n wleidyddol sensitif; ac

– adroddiadau neu lythyron wedi eu drafftio mewn ymateb i gŵyn.

Ceir storio data o'r fath ar liniadur Swyddfa Archwilio Cymru tra bod y gwaith ar y gweill, ond mae'n rhaid ei ddileu oddi ar y gliniadur ar ôl i'r gwaith hwn gael ei gwblhau.

Mae'n rhaid i aelodau staff ystyried ffyrdd diogel o gyfnewid gwybodaeth o'r math hwn, er enghraifft, e-bost wedi'i amgryptio, os gall y derbynnydd bwriadedig ei ddefnyddio. Mae'n dderbyniol hefyd ddefnyddio cof bach wedi'i amgryptio a'i drosglwyddo wyneb yn wyneb.

Ceir defnyddio e-bost rhyngrwyd arferol os na all y derbynnydd bwriadedig ddefnyddio e-bost wedi ei amgryptio, a'i fod yn fodlon derbyn y risg.

c) **Data arall –** hwn yw data nad yw'n perthyn i'r categorïau uchod ac mae'n cynnwys, er enghraifft, gwybodaeth am waith archwilio cyffredinol a chofnodion cyfarfodydd.

Gellir storio'r math hwn o ddata ar liniaduron yn ôl yr angen. Mae'n bosibl defnyddio e-bost rhyngwyd cyffredinol i dderbyn yr wybodaeth hon, neu ei throsglwyddo.

16 Mae'n rhaid i aelodau staff ymgyfarwyddo â gofynion neu bolisïau penodol sydd ar waith mewn corff a archwilir a'u dilyn, er enghraifft, ar gyfer dogfennau wedi'u marcio'n unol â'r system marcio amddiffynnol. Fodd bynnag, os yw gofynion y corff a archwilir yn ymddangos yn rhwymedigaethau diangen sy'n llesteirio mynediad at ddibenion archwilio, dylai aelodau staff godi'r mater â'r rheolwr Cyfraith a Moeseg.

Cof bach (a elwir hefyd yn ffon neu yriant USB)

17 Gellir defnyddio cof bach wedi ei amgryptio, sydd angen cyfrinair i'w ddefnyddio, i drosglwyddo data rhwng cyfrifiaduron, neu i gadw copi wrth gefn. Gellir cael cof bach oddi wrth y tîm TG drwy wneud cais.

18 Mae cof bach cyffredinol nad oes angen cyfrinair arno yn gynhenid beryglus ac ni ddylid ei ddefnyddio byth i gadw data Swyddfa Archwilio Cymru.

Cyfrifiaduron, ffonau clyfar a llechi personol

19 Caiff aelodau staff reoli apwyntiadau calendr a negeseuon e-bost yn eu cyfrifon Swyddfa Archwilio Cymru gan ddefnyddio cyfarpar personol, drwy'r cyfeiriad ar gyfer Outlook ar y we, sef email.wao.gov.uk.

20 Caiff aelodau staff gysylltu eu ffonau clyfar neu eu llechi personol i'w cyfrif e-bost/calendr Swyddfa Archwilio Cymru. I wneud hyn, chwiliwch am yr erthygl 'Defnyddio ffôn clyfar Android neu Apple gydag e-bost neu galendr Swyddfa Archwilio Cymru' ar yr Hub.

Gwneud copi wrth gefn o ddata

21 Gwneir copi wrth gefn o wybodaeth sydd ar systemau a gweinyddion Swyddfa Archwilio Cymru, er enghraifft, Insight, blychau e-bost Outlook, a ffolderi rhwydwaith a rennir, a hynny yn awtomatig. Nid oes angen i aelodau staff gymryd camau arbennig i wneud copïau wrth gefn.

22 Mae'n rhaid i aelodau staff gymryd camau i wneud copi wrth gefn o'r gwaith, pan fo'r unig fersiwn gyfredol ar liniadur yr unigolyn. Er enghraifft, ar ddiwedd y dydd, pan fo aelod o staff wedi bod yn diweddaru adroddiad penodol, dylid arbed y fersiwn ddiweddaraf ar weinydd Swyddfa Archwilio Cymru e.e. y 'P drive', neu ei lanlwytho i'r system Insight. Bydd gwneud hyn yn diogelu rhag colli gwybodaeth os bydd y gliniadur yn methu, a all ddigwydd weithiau yn ddirybudd.

23 Sylwer **na** wneir copïau wrth gefn o 'ffolderi personol', a elwir hefyd yn ffeiliau PST, o fewn Outlook, ar weinyddion yn awtomatig yn yr un modd â'r prif flwch e-bost. Dylai aelodau staff wneud copïau wrth gefn o'r rhain eu hunain os ydynt yn eu defnyddio.

Defnydd derbyniol

24 Ni chaiff staff ddefnyddio cyfarpar Swyddfa Archwilio Cymru mewn unrhyw ffordd a allai niweidio enw da'r sefydliad. Er enghraifft, ni chaniateir i staff anfon, storio neu geisio mynediad bwriadol at ddeunyddiau sydd:

a) yn anweddus neu'n bornograffig;

b) yn debygol o achosi sarhad i lawer;

c) o natur faleisus, ymosodol neu ddifrïol;

d) yn hiliol, yn rhywiaethol neu'n gwahaniaethu yn anghyfreithlon mewn unrhyw ffordd arall yn erbyn nodweddion gwarchodedig fel y'u diffinnir yn Neddf Cydraddoldeb 2010 (h.y. yn ôl oedran, nam (anabledd), ailbennu rhywedd, priodas neu bartneriaeth sifil, beichiogrwydd a chyfnod mamolaeth, hil, crefydd neu gred, rhyw (cenedl) a chyfeiriadedd rhywiol); neu

e) yn gyfystyr ag aflonyddu.

25 Caiff aelodau staff ddefnyddio cyfarpar Swyddfa Archwilio Cymru at ddibenion personol, er enghraifft, i fancio ar-lein, siopa neu ddarllen y newyddion, ar yr amod bod yr amser a dreulir i wneud hyn yn 'egwyl o'r gwaith' sy'n rhesymol fyr.

26 Pan fo'r defnydd personol o gyfarpar Swyddfa Archwilio Cymru yn arwain at gostau, er enghraifft, galwadau personol i ffonau symudol neu ddesg, mae'n rhaid sicrhau nad yw'r gost honno yn ddim mwy na £5 y mis fesul aelod o staff, neu bydd yn rhaid ei had-dalu.

27 Caiff aelodau staff ddefnyddio cyfryngau cymdeithasol, yn amodol ar Bolisi Cyfryngau Cymdeithasol y sefydliad, sydd ar gael ar yr Hub. Yn gyffredinol, dylai aelodau staff fod yn ymwybodol bod y rheolau a'r egwyddorion sy'n gymwys i'r byd go iawn hefyd yn gymwys i'r byd ar-lein.

28 Mae'n rhaid i aelodau staff ymgyfarwyddo â'r gofynion neu'r polisïau penodol sydd ar waith mewn corff a archwilir a'u dilyn wrth ddefnyddio ei gyfrifiaduron neu ei systemau.

Monitro diogelwch

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

30 Bydd Swyddfa Archwilio Cymru yn sicrhau bod y trefniadau monitro yn rhesymol ac yn gymesur â'r risg.

31 Mae'n rhaid i aelodau staff dderbyn y gallai unrhyw ddefnydd o gyfarpar Swyddfa Archwilio Cymru gael ei recordio, pa un a yw at ddefnydd busnes neu ddefnydd personol, a hefyd gellir craffu arno a'i archwilio drwy ddulliau awtomatig neu fel arall.

Rhoi gwybod am ddigwyddiadau diogelwch

32 Mae'n rhaid i aelodau staff roi gwybod i'r desg gymorth TG am unrhyw ddigwyddiadau diogelwch. Gallai'r rhain gynnwys digwyddiadau pan fo, e.e, aelodau staff corff sy'n cael ei archwilio wedi anfon gwybodaeth bersonol a sensitif drwy e-bost rhyngrwyd cyffredin, neu pan fo gliniadur wedi'i ddwyn. Drwy roi gwybod am y digwyddiadau yn brydlon, dylai fod modd cymryd camau unioni gan helpu Swyddfa Archwilio Cymru a chyrff eraill i ddysgu a gwneud unrhyw newidiadau angenrheidiol i atal yr un peth rhag digwydd eto.

33 Bydd y ddesg gymorth TG yn trosglwyddo gwybodaeth am unrhyw ddigwyddiad i'r Swyddog Diogelu Gwybodaeth ac i'r Pennaeth Cyfraith a Moeseg, a fydd yn cydweithio i ymdrin â'r digwyddiad. Bydd yr adran Cyfraith a Moeseg yn asesu ac yn cofnodi'r digwyddiad ac yn ystyried camau dilynol yn unol â rhestr wirio mynediad diawdurdod at ddata, gan gynnwys unrhyw gyfathrebu angenrheidiol â rhanddeiliaid mewnol ac allanol, ac â Swyddfa'r Comisiynydd Gwybodaeth.

Dod o hyd i gymorth

34 Os oes angen cyngor arnoch ar unrhyw fater yn y polisi hwn, neu'n ymwneud ag unrhyw agwedd ymarferol ar weithio gyda gwybodaeth ar gyfarpar Swyddfa Archwilio Cymru, cysylltwch â'r tîm TG ar 02920 320690 neu anfonwch e-bost i 'Wales Audit Office ICT'.