Cyfeirnod: Fersiwn 3.5
Dyddiad cyhoeddi: Gorffennaf 2024
Cyswllt allweddol: Matthew Jubb

Polisi Diogelwch Gwybodaeth

Cynnwys

Hanes adolygu

Fersiwn	Crynodeb o'r newidiadau	Dyddiad
F1.0	Fersiwn gyntaf wedi'i chwblhau.	Chwefror 2006
F1.1	Newid i'r Swyddog Diogelwch Gwybodaeth, wedi diwygio paragraff 29 fel bod cysylltu â rhwydwaith band eang yn y cartref yn cael ei ganiatáu.	Hydref 2007
F2.0	Adolygiad mawr gan gynnwys canllawiau manylach ynghylch 'gofalu am offer' a 'chael data busnes gan gyrff a archwilir'.	Hydref 2008
F2.1	Newid i adlewyrchu'r ffaith 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 ac o dan glo yn y gist, neu mewn man cyfatebol.	Mai 2009
F2.2	Adolygu'r adran ar Fonitro a Gorfodi Diogelwch, gan egluro y bydd monitro rheolaidd yn digwydd. Bydd y gweithgarwch monitro'n gwirio sut y mae staff yn cydymffurfio â'r gyfraith a'r Polisi Diogelwch Gwybodaeth yma. Mynediad at wefannau rhwydweithio cymdeithasol ac e-bost allanol wedi'i wahardd.	Gorffennaf 2010
F2.3	Cynnwys deunydd i ddarparu eglurhad o ddefnydd derbyniol o gyfleusterau prosesu gwybodaeth. Cynnwys atodiad 3 newydd yn nodi polisi monitro rheolaidd manwl.	Medi 2011
F3.0	Adolygiad 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 y gellir trosglwyddo data gan ddefnyddio ffeiliau Microsoft a ddiogelwyd â chyfrinair cryf.	Chwefror 2018
F3.3	Newidiadau i ddiffinio categorïau data'n fwy eglur.	Mai 2018
F3.4	Eglurhad o ddefnyddio a diogelu dyfeisiau personol	Mawrth 2020
F3.5	Wedi'i olygu er mwyn darllenadwyedd, wedi tynnu cyfeiriadau at enwau hen gynhyrchion, e.e. Skype, Insight, allan a disodli "Swyddfa Archwilio Cymru" ag "Archwilio Cymru". Wedi diweddaru'r canllawiau ynghylch cofau bach. Wedi diweddaru'r canllawiau ynghylch cyfrineiriau, defnyddio gliniaduron wrth deithio, cyfarpar diogelu sgrîn.	Gorffennaf 2024

Crynodeb

1 Mae'r gofynion yn y polisi hwn yn berthnasol i'r holl gyflogeion, aelodau anweithredol a chontractwyr, pa un a ydynt yn cael eu cyflogi trwy asiantaeth, ynteu'n uniongyrchol. Er mwyn 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 i gadw gwybodaeth y sefydliad yn ddiogel.

3 Er bod y polisi hwn yn cynnwys ffocws ymarferol ar ddiogelwch gwybodaeth, dylid ei ddarllen ar y cyd â'r Polisi Llywodraethu Gwybodaeth (gan gynnwys y Polisi Diogelu Data), dogfen gynhwysfawr 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 sicrhau eu bod wedi darllen a deall y cynnwys.

5 Mae'r ddogfen hon yn cynnwys polisi swyddogol y sefydliad. Dangosir yr hanes adolygu ar y ddalen eglurhaol.

System Rheoli Diogelwch Gwybodaeth

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

- mynd ati'n systematig i archwilio ac asesu'r risgiau i ddiogelwch gwybodaeth Archwilio Cymru, gan ystyried bygythiadau, gwendidau ac effeithiau;
- dylunio a gweithredu cyfres gydlynol a chynhwysfawr o reolaethau diogelwch gwybodaeth a/neu ffyrdd eraill o drin risgiau i sicrhau bod risgiau'n cael eu lleihau i lefel dderbyniol, gan gynnwys disodli neu ddiweddaru systemau sydd wedi datblygu gwendidau seiber, a pharatoi rhag blaen i hwyluso adferiad, pe bai ymosodiad seiber yn digwydd;
- mabwysiadu proses reoli drosfwaol i sicrhau bod y rheolaethau diogelwch gwybodaeth yn dal i ddiwallu anghenion diogelwch gwybodaeth y sefydliad yn barhaus.

Cyfrifoldebau staff

Enwau defnyddwyr a chyfrineiriau

7 Bydd pob aelod o staff yn cael cyfuniad o enw defnyddiwr a chyfrinair i'w ddefnyddio gyda systemau Archwilio Cymru, er enghraifft wrth fewngofnodi ar liniadur, neu adfer slip cyflog misol. Gofynnir i gydweithwyr newid y cyfrinair yn eu sesiwn gynefino TG. Ni ddylai'r cyfrineiriau hynny gael eu rhannu gyda

chydweithwyr. Cysylltwch â'r tîm TG os nad ydych yn gallu cael mynediad at y systemau neu'r adnoddau y mae angen i chi gael mynediad atynt.

8 Dylai cyfrineiriau fod yn gofiadwy, ac ni ddylid byth eu hysgrifennu i lawr. Chwiliwch ar Google am "NCSC three random words" i gael canllawiau gan y Ganolfan Seiberddiogelwch Genedlaethol ynghylch sut i ddewis cyfrinair cryf sy'n hawdd i'w gofio.

9 Ni ddylech ddefnyddio'r un cyfrinair ag sydd gennych ar unrhyw gyfrifon personol yr ydych yn eu defnyddio, e.e. Amazon, Gmail, Ebay a.y.b.

Cysylltu offer personol neu offer nad yw'n eiddo i Archwilio Cymru

10 Gall ffonau clyfar neu gyfrifiaduron personol neu rai o eiddo ymwelwyr gael eu cysylltu â'r rhyngrwyd trwy WiFi Archwilio Cymru i westeion, neu yng Nghyffordd Llandudno, WiFi Llywodraeth Cymru i westeion – chwiliwch am 'WiFi i westeion' ar yr Hwb am fanylion. Ni ddylai offer nad yw'n eiddo i Archwilio Cymru gael ei gysylltu mewn unrhyw ffordd arall – er enghraifft â chebl rhwydwaith.

Gofalu am offer a gwybodaeth

11 Er bod data ar liniaduron a ffonau clyfar Archwilio Cymru'n cael ei ddiogelu trwy amgryptio, rhaid i staff gymryd gofal rhesymol am offer Archwilio Cymru. Rhaid i staff hefyd gymryd pob gofal rhesymol am wybodaeth Archwilio Cymru a gaiff ei phrosesu ar ddyfeisiau personol neu a gaiff ei dal ar bapur. Os yw offer neu wybodaeth Archwilio Cymru'n cael ei d(d)wyn neu ei g/cholli oherwydd methiant i gymryd gofal rhesymol bydd hynny'n cael ei drin fel mater difrifol.

12 Rhaid i staff beidio â gadael offer neu wybodaeth Archwilio Cymru heb neb i ofalu amdano/amdani lle ceir risg y bydd yn cael ei d(d)wyn – er enghraifft ar agor (h.y. sgrîn heb ei chloi) ar y bwrdd wrth deithio ar drên, neu mewn ystafell gyfarfod heb ei chloi mewn gwesty yn ystod egwyl cinio.

13 Rhaid i wybodaeth gyfrinachol sy'n gysylltiedig â gwaith gael ei diogelu ac felly rhaid i staff fod yn ofalus ynglŷn â sgrîn eu gliniadur yn bod yn weladwy i eraill. Wrth deithio, ni ddylai staff weithio ar faterion neu ddogfennau cyfrinachol gyda data personol pan fo risg y bydd eu sgrîn yn cael ei gweld.

14 Rhaid i staff gloi sgrîn eu gliniadur wrth gamu i ffwrdd oddi wrth eu gliniadur, pa un a ydynt yn gweithio mewn swyddfa, ynteu'n gweithio gartref neu mewn lleoliadau eraill. Os oes angen busnes am gyfarpar diogelu sgrîn (sy'n helpu i atal gwybodaeth rhag bod yn weladwy i eraill), er enghraifft os yw swyddfa'n cael ei rhannu gyda staff o gorff arall, rhaid i staff gysylltu â'r tîm TG gyda'u cais.

15 Gellir gadael offer neu wybodaeth Archwilio Cymru mewn car heb neb i ofalu amdano/amdani am hyd at 4 awr, ar yr amod ei f/bod yn cael ei (g)adael o'r golwg a bod y car wedi'i gloi – ond byth dros nos.

16 Gall staff adael offer neu wybodaeth Archwilio Cymru heb neb i ofalu amdano/amdani ar safleoedd swyddfeydd lle ceir ‘diogelwch terfynau’ rhesymol h.y. mesurau i atal pobl heb awdurdod rhag mynd i mewn i’r swyddfa, neu gartref.

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

Cael a chyfleu gwybodaeth

18 Mae Archwilio Cymru’n rhannu gwybodaeth yn dri chategori. Mae gwahanol ragofalon trin 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 gofid neu niwed difrifol i unigolion neu niwed difrifol i enw da neu fuddiannau Archwilydd Cyffredinol Cymru, Archwilio Cymru neu bartïon eraill megis cyrff a archwilir, Gweinidogion Cymru a Chynulliad Cenedlaethol Cymru.** Bydd hyn yn cynnwys gwybodaeth trethdalwyr, fel a ddiffinnir gan Ddeddf Casglu a Rheoli Trethi (Cymru) 2016, ac unrhyw ddata personol arwyddocaol, er enghraifft gwybodaeth a gyflwynir gan 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 yn dilyn adolygiad gan Swyddog Diogelu Data Archwilio Cymru a fydd yn cynghori ynghylch y mesurau diogelwch sy’n ofynnol a, lle y bo’n briodol, yn cysylltu â’r Swyddog Diogelu Data yn y corff a archwilir.

b. **Data sensitif – gwybodaeth sydd â’r potensial i gael effaith negyddol ar unigolion neu fuddiannau neu enw da Archwilydd Cyffredinol Cymru, 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 gan y wasg ddiddordeb 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 Archwilio Cymru am gyhyd ag y mae gwaith yn cael ei wneud 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 e-bost wedi’i amgryptio, os yw’r derbynnydd bwriadedig yn gallu defnyddio’r dull yma.

c. **Data arall –** mathau o ddata nad ydynt wedi'u cynnwys yn y categorïau uchod yw'r rhain ac maent yn cynnwys, er enghraifft, gwybodaeth weithio gyffredinol sy'n ymwneud ag archwiliadau a chofnodion cyfarfodydd.

   Gall y math yma o ddata gael ei storio ar liniaduron fel y bo'n ofynnol. Fel arfer, gellir defnyddio e-bost rhyngrwyd i'w gaffael 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 dilyn y gofynion neu'r polisïau hynny, er enghraifft ar gyfer dogfennau â marc diogelwch. Fodd bynnag, os ymddengys fod gofynion corff a archwilir yn rhy feichus fel eu bod yn rhwystr i fynediad at ddibenion archwilio, dylai staff godi'r mater gyda thîm y Gyfraith a Moeseg.

Cofau bach (a adwaenir hefyd fel cofau neu yriannau USB)

20 Fel dewis diofyn, mae cofau bach wedi'u rhwystro ar liniaduron Archwilio Cymru. Os ydych yn ystyried defnyddio cof bach at unrhyw ddiben, cysylltwch â'r Tîm TG i gael cyngor.

Defnyddio eich "dyfeisiau eich hunain" fel ffonau clyfar personol ar gyfer gwaith Archwilio Cymru

21 Mae Archwilio Cymru'n derbyn ei bod hi'n gyfleus ac yn effeithiol i'r sefydliad (yn ogystal â staff), bod staff yn defnyddio'u dyfeisiau eu hunain ar gyfer gwaith Archwilio Cymru. Fodd bynnag, mae Archwilio Cymru yn dal i fod yn gyfrifol am brosesu ei ddata, hyd yn oed os gwneir hynny ar ddyfeisiau o'r fath. Felly wrth brosesu data Archwilio Cymru, megis defnyddio ap Outlook Archwilio Cymru ar gyfer e-bost, ar ddyfeisiau staff eu hunain, rhaid dilyn gofynion y Polisi Llywodraethu Gwybodaeth a'r adrannau "Cyfrifoldebau Staff" a "Rhoi gwybod am ddigwyddiadau diogelwch" yn y polisi hwn. Rhaid i staff wneud pob ymdrech resymol i sicrhau bod yr wybodaeth o eiddo 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*** Archwilio Cymru ar yr Hwb i wirio a yw'r modd y maent yn defnyddio'u dyfais yn ddigon diogel ac, os oes angen, cael cyngor gan y tîm TG.

Creu copïau wrth gefn o ddata

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

23 Rhaid i staff gymryd gamau i greu copïau wrth gefn o waith, os mai copi ar liniadur unigolyn yw'r unig gopi cyfoes. Er enghraifft, ar ddiwedd diwrnod pan fo aelod o

staff wedi bod yn diweddaru adroddiad penodol, dylai'r fersiwn ddiweddaraf gael ei chadw ar Sharepoint. Bydd hyn yn gochel rhag colli gwybodaeth os bydd y gliniadur yn methu, sy'n gallu digwydd yn achlysurol heb rybudd.

Defnydd derbyniol

24 Ni ddylai staff ddefnyddio offer Archwilio Cymru mewn unrhyw ffordd a all niweidio enw da'r sefydliad. Er enghraifft, ni ddylai staff anfon, storio na chael mynediad yn fwriadol at ddeunydd sydd:

a. yn anllad neu'n bornograffig;

b. yn debygol o beri tramgwydd cyffredin;

c. yn faleisus, yn ddifrïol neu'n ddifenwol o ran ei natur;

d. yn hiliol, rhywiaethol neu'n gyfystyr fel arall â chamwahaniaethu ar sail 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

e. yn gyfystyr ag aflonyddu.

25 Gall staff ddefnyddio offer 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 'egwyl o'r gwaith' sy'n gymharol fyr. Mae gwebost personol ar liniaduron wedi'i rwystro am resymau seiberddiogelwch.

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

27 Gall staff ddefnyddio'r cyfryngau cymdeithasol, yn amodol ar Bolisi Cyfryngau Cymdeithasol y sefydliad, sydd ar yr Hwb. Yn gyffredinol, dylai staff fod yn ymwybodol y byddai rheolau ac egwyddorion ymddygiad y byd go iawn yn berthnasol yn y byd ar-lein hefyd.

28 Rhaid i staff eu gwneud eu hunain yn ymwybodol o unrhyw ofynion neu bolisïau penodol sydd gan gorff a archwilir a dilyn y gofynion neu'r polisïau hynny wrth ddefnyddio'i gyfrifiaduron neu systemau. Mae canllawiau ar gael ar fynediad o bell yn yr adran o'r fframwaith Sgiliau Digidol sy'n ymwneud â 'thrin gwybodaeth'.

29 Gwaherddir staff rhag trosglwyddo gwybodaeth a gafwyd wrth wneud eu gwaith y tu allan i'r parth gwaith i dderbynyddion neu ddyfeisiau anawdurdodedig, gan gynnwys eu system e-bost neu ddyfais storio eu hunain. Byddai'r trosglwyddiadau hyn yn gyfystyr â phrosesu gwybodaeth heb awdurdod ac fe allent arwain at danseilio diogelwch data personol. Mae'r gwaharddiad hwn yn berthnasol yn ystod

cyflogaeth, yn ystod cyfnod rhybudd ar gyfer ymadawyr ac ar ôl i gyflogaeth ddod i ben.[1]

Monitro diogelwch

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

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

32 Rhaid i staff dderbyn y gall unrhyw ddefnydd o offer Archwilio Cymru, boed yn ddefnydd busnes neu'n ddefnydd personol, gael ei recordio, ac y gellir craffu arno neu ymchwilio iddo trwy'r dulliau awtomataidd neu'r dulliau â llaw hyn.

Rhoi gwybod am ddigwyddiadau diogelwch

33 Rhaid i staff roi gwybod i'r ddesg gymorth TG am ddigwyddiadau diogelwch. Gallai'r rhain gynnwys achosion, er enghraifft, lle mae staff corff a archwilir wedi anfon gwybodaeth bersonol a sensitif trwy e-bost rhyngrwyd cyffredin, neu lle mae gliniadur wedi cael ei golli neu ei ddwyn. Dylai rhoi gwybod yn brydlon ei gwneud yn bosibl cymryd camau cywirol a helpu Archwilio Cymru a chyrff eraill i ddysgu a gwneud unrhyw newidiadau angenrheidiol i osgoi digwyddiad arall tebyg.

34 Bydd y ddesg gymorth TG yn hysbysu'r Swyddog Diogelwch Gwybodaeth a Phennaeth y Gyfraith a Moeseg am unrhyw ddigwyddiad, a byddant hwythau'n cynnal cyswllt mewn perthynas ag ymdrin â'r digwyddiad hwnnw. Bydd tîm y Gyfraith a Moeseg yn asesu ac yn cofnodi'r digwyddiad ac yn ystyried y camau nesaf yn unol â'r rhestr wirio diogelu data, sy'n cynnwys asesu lefel y risg a achosir gan y digwyddiad. Bydd y Swyddog Diogelu Data'n rhoi cyngor ynghylch y cwestiwn a yw diogelwch data wedi cael ei danseilio ac a oes angen rhoi gwybod i Swyddfa'r Comisiynydd Gwybodaeth am hyn.

Cael help

35 Os oes arnoch angen cyngor ynghylch unrhyw beth yn y polisi hwn, neu unrhyw agwedd ymarferol ar weithio gyda gwybodaeth ar offer Archwilio Cymru, cysylltwch

[1] **Mae'r Polisi Llywodraethu Gwybodaeth yn nodi'r gofynion ar gyfer trin gwybodaeth a diogelu data, ac mae'r Cod Ymarfer ar gyfer Staff a chontractau cyflogaeth yn nodi gofynion mewn perthynas â chyfrinachedd.**

â'r tîm TG ar 02920 320690, anfonwch neges e-bost at "Cymorth TG" neu cysylltwch ag aelod o'r tîm yn uniongyrchol dros Teams.