WHC (2017) 025

CYLCHLYTHYR IECHYD CYMRU

Llywodraeth Cymru
Welsh Government

Dyddiad Cyhoeddi: 4 Gorffennaf 2017

STATWS: GWEITHREDU

CATEGORI: LLYWODRAETHU GWYBODAETH

Teitl: Arweiniad ar Seiberddiogelwch a'r gofynion Llywodraethu Gwybodaeth i gwmnïau cyflenwi a'r gadwyn gyflenwi

Dyddiad Dod i Ben / Adolygu Amh

I'w weithredu gan:
Ymddiriedolaethau a byrddau iechyd

Gweithredu yn ofynnol erbyn: Ar unwaith

Anfonir gan: Dr Andrew Goodall, Cyfarwyddwr Cyffredinol Iechyd a Gwasanaethau Cymdeithasol / Prif Weithredwr GIG Cymru

Enw(au) Cyswllt yn AIGC Llywodraeth Cymru:
Peter Jones, Dirprwy Gyfarwyddwr, Iechyd a Gofal Digidol, Grŵp Iechyd a Gwasanaethau Cymdeithasol, Parc Cathays, Caerdydd, CF10 3NQ

E-bost: HSS-DHCMailbox@wales.gsi.gov.uk

Wedi'i amgáu: Dim

WHC 2017/025 – Arweiniad ar Seiberddiogelwch a'r gofynion Llywodraethu Gwybodaeth i gwmnïau cyflenwi a'r gadwyn gyflenwi.

Gyda bygythiadau seiberddiogelwch yn cynyddu fwyfwy, mae angen i GIG Cymru sicrhau bod y gofynion a roddir ar gwmnïau cyflenwi, a'r gadwyn gyflenwi gyfan o bosibl, yn dal i fod yn briodol i lefel y wybodaeth y caiff y cwmni cyflenwi fynediad iddi a/neu a ddelir ganddo.

Rhaid i bob sefydliad fod yn ymwybodol o'r holl drydydd partïon sy'n dal, yn gweld neu'n trafod data adnabyddadwy am staff neu gleifion, a sicrhau bod y lefel sicrwydd briodol yn cael ei dangos a'i chynnal yn barhaus. Dylid gwneud hyn o safbwynt y data a'r contract gyda'r cwmni cyflenwi.

Dylai'r holl reolyddion gael eu hadolygu'n rheolaidd a'u diweddaru i adlewyrchu deddfwriaeth newydd neu ddiwygiedig ac unrhyw arferion gorau diwygiedig sy'n cael eu rhyddhau gan arbenigwyr y diwydiant.

Os yw'r broses o gaffael ac wedyn cyflenwi unrhyw nwyddau, gwasanaethau neu offer yn arwain at un neu ragor o'r amodau a restrir isod, rhaid i reolyddion seiberddiogelwch a llywodraethu gwybodaeth priodol gael eu dynodi yn y gofynion a rhaid iddynt fod ar waith mewn unrhyw gytundebau contractiol neu fasnachol dilynol (h.y. yn y set briodol o delerau ac amodau ar gyfer y contract):

- Pan fydd y cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, yn storio neu'n prosesu gwybodaeth am gleifion, staff neu wybodaeth bersonol sensitif arall; neu
- Pan fydd gan y cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, fynediad i systemau ar rwydwaith y GIG sy'n storio neu'n prosesu gwybodaeth am gleifion, staff neu wybodaeth bersonol sensitif arall.

Rhaid i dimau caffael gydweithio â'r arbenigwyr seiberddiogelwch a llywodraethu gwybodaeth priodol yn eu sefydliad neu ar lefel genedlaethol (h.y. o fewn Gwasanaeth Gwybodeg GIG Cymru) i sicrhau y cyflawnir/y glynir wrth hyn.

Mae Atodiad A yn cynnig fframwaith asesu risg er mwyn asesu pob contract trydydd parti yn ei erbyn ynghyd â'r safonau seiberddiogelwch gofynnol y dylid eu gweithredu.

Isod ceir yr ystyriaethau gofynnol argymelledig sy'n ymwneud â Llywodraethu Gwybodaeth:

- Cydymffurfio ag offer Egwyddorion Caldicott ar Waith (CPIP) Cymru neu Becyn Cymorth Llywodraethu Gwybodaeth Lloegr;
- Cymalau cyfrinachedd a diogelu data cadarn yn y contractau;
- Cydymffurfio â darpariaethau *Safe Harbour* neu'r *Privacy Shield* newydd rhwng yr UE ac UDA ar gyfer trosglwyddo unrhyw ddata i'r Unol Daleithiau; a
- Chydymffurfio ag arweiniad Swyddfa'r Comisiynydd Gwybodaeth (ICO) ar ddelio ag achos o fynediad heb ei awdurdodi at ddata.

Mae Atodiad B ac C yn darparu crynodeb o'r ddwy ffurf ar gontractau y mae Gwasanaeth Gwybodeg GIG Cymru (NWIS) yn eu defnyddio i gaffael nwyddau a gwasanaethau cysylltiedig â TG. Mae gwybodaeth bellach am y rhain i'w cael oddi wrth Dîm Gwasanaethau Masnachol NWIS.

Os oes gennych unrhyw gwestiynau am y cylchlythyr hwn, dylech gysylltu ag:

Iechyd a Gofal Digidol
4ydd Llawr
Grŵp Iechyd a Gwasanaethau Cymdeithasol
Parc Cathays
Caerdydd
CF10 3NQ

E-bost: DHSS-DigitalHealthandCare@Wales.GSI.Gov.UK

Yn gywir

Dr Andrew Goodall

ATODIAD A

Safonau gofynnol ar gyfer rheolyddion Seiberddiogelwch

Isod, ceir y rheolyddion Seiberddiogelwch gofynnol y dylid eu defnyddio, yn ddibynnol ar y lefel asesedig o risg i systemau/data.

1. Amherthnasol

Yn y senario hwn, nid yw'r cwmni cyflenwi, nac unrhyw barti yn ei gadwyn gyflenwi, yn storio, prosesu nac yn gweld gwybodaeth am gleifion, staff na gwybodaeth bersonol sensitif arall, ac nid oes ganddo fynediad i wybodaeth gorfforaethol sensitif.

Nid oes gan y cwmni cyflenwi, nac unrhyw barti yn ei gadwyn gyflenwi, unrhyw fath o gysylltiad electronig / wedi'i rwydweithio â dyfeisiau ar rwydwaith GIG Cymru, gan gynnwys cysylltu â rhwydweithiau/dyfeisiau pan mae eu staff ar safleoedd y GIG.

Y mathau o gontractau y mae hyn yn debygol o fod yn berthnasol iddo ydy rhai sy'n gyfrifol am brynu nwyddau neu ddarpariaethau gwasanaethau safonol (e.e. cyflenwadau swyddfa neu waredu gwastraff nad yw'n wastraff sensitif).

Nid oes i'r categori hwn unrhyw fesurau rheoli seiberddiogelwch gofynnol penodol, er hynny, fe argymhellir bod pob cyflenwr yn ceisio sicrhau ei fod yn cydymffurfio â'r Cynllun Hanfodion Seiber, sy'n golygu bod y cyflenwr yn gwneud hunanasesiad anffurfiol ac yn ymrwymo i wella diogelwch.

2. Isel Iawn (VL)

Yn y senario hwn, nid yw'r cwmni cyflenwi, nac unrhyw barti yn ei gadwyn gyflenwi, yn storio, prosesu nac yn gweld gwybodaeth am gleifion, staff na gwybodaeth bersonol sensitif arall, ac nid oes ganddo fynediad i wybodaeth gorfforaethol sensitif.

Mae ar y cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, angen mynediad anaml ad-hoc i ddyfeisiau sydd wedi'u cysylltu â rhwydwaith GIG Cymru, neu i'r rhwydwaith ei hun, a fyddai'n digwydd drwy fynychu safleoedd a chysylltu'n uniongyrchol â'r offer.

Gallai'r mathau o gontractau y gallai hyn yn fod yn berthnasol iddo gynnwys cwmnïau cynnal a chadw adeiladau, cwmnïau cynnal a chadw peiriannau argraffu, cyflenwyr meddalwedd arbenigol, anghlinigol, neu debyg.

Yn y categori hwn, aseswyd mai risgiau seiberddiogelwch sylfaenol y bydd y contract yn eu peri i GIG Cymru (h.y. hacio syml/awtomataidd, gwe-rwydo neu ysbïwedd) ac mae unrhyw ymosodwr yn debygol o fod yn fanteisgar, yn ddi-sgil ac anfynych. Mae effaith dwyn/colli data ar y sefydliad yn y GIG (ymddiriedaeth gyhoeddus, dirwyon ariannol, ayb) yn debygol o fod yn isel.

Mae'r lefel hon yn mynnu bod y contractwr yn cydymffurfio â'r Cynllun Hanfodion Seiber, sy'n golygu bod y contractwr yn gwneud hunan-asesiad ffurfiol, yn datgan ei fod yn cydymffurfio, a bod corff ardystiedig yn dilysu'r ddogfennaeth.

3. Isel (L)

Yn y senario hwn, gallai'r cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, gael mynediad i ychydig iawn o wybodaeth am gleifion, staff neu wybodaeth bersonol sensitif arall sy'n cael ei storio ar rwydwaith y GIG, neu fynediad cyfyngedig iawn i wybodaeth gorfforaethol sensitif. Ni chaiff ddim o'r cyfryw wybodaeth ei storio gan y cwmni cyflenwi, nac unrhyw barti yn ei gadwyn gyflenwi.

Mae hefyd yn bosibl y bydd gofyn i'r cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, gael mynediad anaml ad-hoc i ddyfeisiau sydd wedi'u cysylltu â rhwydwaith GIG Cymru, neu'r rhwydwaith ei hun, a fyddai'n digwydd drwy fynychu safleoedd a chysylltu'n uniongyrchol â'r offer. Ni fydd dim modd o gael mynediad i unrhyw systemau sydd wedi'u cysylltu â rhwydwaith y GIG, nac unrhyw ddata a ddelir ar systemau'r GIG o bell.

Yn y categori hwn, aseswyd y gallai'r bygythiad fod wedi'i dargedu ychydig mwy (h.y. yn cynnwys gwe-rwydo wedi'i dargedu neu feddalwedd wystlo a lle bo'r ymosodwyr yn lled-sgilgar ond ddim yn fynych o bosibl). Mae effaith dwyn/colli data ar yr unigolion a'r sefydliad GIG dan sylw (ymddiriedaeth gyhoeddus, dirwyon ariannol, ayb) yn debygol o fod yn isel.

Mae'r lefel hon yn mynnu bod y contractwr yn cydymffurfio â'r Cynllun Hanfodion Seiber, sy'n golygu bod y contractwr yn gwneud hunan-asesiad ffurfiol, yn datgan ei fod yn cydymffurfio, a bod corff ardystiedig yn dilysu'r ddogfennaeth.

4. Cymedrol (M)

Yn y senario hwn, mae gan y cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, fynediad i fwy o ddata personol, neu i ddata personol mwy sensitif yn ymwneud â staff neu gleifion, neu fynediad i wybodaeth gorfforaethol sensitif. Gallai'r wybodaeth hon fod yn cael ei storio a'i phrosesu ar rwydwaith/ systemau'r GIG neu gan y cwmni cyflenwi, neu un o'r partïon yn ei gadwyn gyflenwi.

Gellid bod ar y cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, hefyd angen mynediad aml i ddyfeisiau sydd wedi'u cysylltu â rhwydwaith GIG Cymru, neu'r rhwydwaith ei hun, a fyddai'n digwydd naill ai drwy fynychu safle a chysylltu'n uniongyrchol, neu drwy gyfrwng peirianwaith mynediad o bell awdurdodedig.

Mae'r categori cymedrol yn berthnasol i gontractau lle'r aseswyd bod y risgiau seiber yn fwy datblygedig. Mae hwn yn debygol o fod yn berthnasol i gontractau lle ceir mwy o ddata personol sensitif neu ddata personol mwy sensitif. Mae'r ymosodiadau'n debygol o fod wedi'u targedu gyda'r nod o gael mynediad i ased(au) penodol neu i atal gwasanaethau. Mae'r ymosodwr yn debygol o fod yn fynych, yn drefnus a naill ai'n sgilgar neu â mynediad i sgiliau (e.e. seiberdroseddwyr neu hacwyr ymgyrchu). Mae effaith dwyn/colli data ar yr unigolion a'r sefydliad GIG dan sylw (ymddiriedaeth gyhoeddus, dirwyon ariannol, ayb) yn debygol o fod yn gymedrol.

Mae'r lefel hon yn mynnu bod y contractwr yn cael ac yn cynnal Ardystiad Hanfodion Seiber a Mwy, sy'n golygu bod y contractwr yn gwneud hunan-asesiad ffurfiol, yn datgan ei fod yn cydymffurfio, a bod corff ardystiedig yn dilysu'r ddogfennaeth.

Er mwyn ennill a chynnal ardystiad, mae angen i gontractwyr hefyd gael prawf i weld pa mor agored i niwed ydynt (gan sefydliad profi allanol cymwysedig / ardystiedig priodol), ac ail-ardystio yn erbyn Hanfodion Seiber a Mwy o leiaf unwaith y flwyddyn.

5. Uchel (H)

Mae'r categori Risg Seiber Uchel yn berthnasol i gontractau sy'n hanfodol i gefnogi gallu clinigol allweddol a'r rheini sy'n delio â data personol, sensitif swmpus am staff neu gleifion, neu sydd â mynediad i wybodaeth gorfforaethol gyfrinachol iawn. Gallai'r wybodaeth hon fod yn cael ei storio a'i phrosesu ar rwydwaith/ systemau'r GIG neu gan y cwmni cyflenwi, neu un o'r partïon yn ei gadwyn gyflenwi.

Gellid bod ar y cwmni cyflenwi, neu unrhyw barti yn ei gadwyn gyflenwi, hefyd angen mynediad aml i ddyfeisiau sydd wedi'u cysylltu â rhwydwaith GIG Cymru, neu'r rhwydwaith ei hun, a fyddai'n digwydd naill ai drwy fynychu safle a chysylltu'n uniongyrchol, neu drwy gyfrwng peirianwaith mynediad o bell awdurdodedig.

Mae'r categori uchel yn berthnasol i gontractau lle'r aseswyd bod y risgiau seiber i'r contract yn Fygythiadau Mynych Datblygedig. Bydd ymosodwyr ar y lefel hon fel arfer yn drefnus, yn soffistigedig iawn, yn fynych a bydd ganddynt ddigonedd o adnoddau. Gallai'r ymosodiadau fod yn estynedig dros amser hir a gallent fod yn segur am fisoedd neu flynyddoedd ar ôl yr ymosodiad cychwynnol. Mae effaith dwyn/colli data ar yr unigolion a'r sefydliad GIG dan sylw (ymddiriedaeth gyhoeddus, dirwyon ariannol, ayb) yn debygol o fod yn sylweddol.

Mae'r lefel hon yn mynnu bod y contractwr yn cael ac yn cynnal Ardystiad Hanfodion Seiber a Mwy, sy'n golygu bod y contractwr yn gwneud hunan-asesiad ffurfiol, yn datgan ei fod yn cydymffurfio, a bod corff ardystiedig yn dilysu'r ddogfennaeth.

Er mwyn cael a chynnal ardystiad, mae angen i gontractwyr hefyd gael prawf i weld pa mor agored i niwed ydynt (gan sefydliad profi allanol cymwysedig / ardystiedig priodol), ac ailardystio yn erbyn Hanfodion Seiber a Mwy o leiaf unwaith y flwyddyn.

Yn ogystal â chynnal Ardystiad Hanfodion Seiber a Mwy, disgwylir i'r contractwr hefyd brofi ei fod yn gweithio i ennill ardystiad yn erbyn safon ISO/IEC 27001:2013, sy'n rhoi sicrwydd ychwanegol ynglŷn ag ymrwymiad parhaus y contractwr i wella diogelwch.

ATODIAD B

Telerau ac Amodau Cymhleth

Model Cymhleth – Gwasanaeth Masnachol y Goron (OGC gynt) Contract TGCh a Gwasanaethau Model ar gyfer atebion a gwasanaethau TG gwerth dros £10m. Mae'r math hwn o gontract yn adlewyrchu blaenoriaethau presennol y llywodraeth a'r ffyrdd a argymhellir o gynnal busnes a chaiff ei gywreinio'n seiliedig ar yr ateb/gwasanaeth sy'n cael ei gaffael. Fodd bynnag, dyma'r telerau allweddol:

Telerau Contractiol Allweddol Llywodraethu Gwybodaeth:

- Cydymffurfio â'r Ddeddf Diogelu Data a'r 7fed a'r 8fed Egwyddor;
- Diogelu Data Personol;
- Ym mha amgylchiadau y gall y contractwr ddefnyddio Data Personol i gyflawni'r cytundeb;
- Defnyddio rhannu a defnyddio data o safbwynt y Ddeddf Rhyddid Gwybodaeth; a
- Chyfrinachedd gwybodaeth.

Telerau Contractiol Allweddol Diogelwch

- Personél y Contractwr yn cydymffurfio â'r Cynllun a'r Gofynion Diogelwch a'r Polisi Diogelwch;
- Yr Awdurdod i hysbysu o unrhyw newidiadau yn y Polisi Diogelwch; a
- Chydymffurfio â'r Atodlen Diogelwch (Atodlen 2.4) a'r Safonau (Atodlen 2.3)

Ceir atodlenni penodol dan Delerau ac Amodau'r Contract, sy'n disgrifio'n fanwl y darpariaethau a'r rhwymedigaethau contractiol ar gyfer Llywodraethu Gwybodaeth a Diogelwch.

Atodlen 2.3 Safonau (Diogelwch a Llywodraethu Gwybodaeth)
Yn datgan y safonau y mae'n rhaid glynu wrthynt wrth gyflenwi'r gwasanaeth e.e. Safon Ddiogelwch ISO 27001.

Atodlen 2.4 Gofynion Diogelwch (Diogelwch)
Yn datgan yr egwyddorion diogelwch ar gyfer y feddalwedd, yr agweddau ehangach ar ddiogelwch o ran proses yr ateb/ gwasanaeth ar gyfer creu'r Cynllun Diogelwch ac archwilio a phrofi'r Cynllun Diogelwch.

Atodlen 2.5 Parhad Busnes (Diogelwch)
Yn datgan gofynion yr awdurdod ar gyfer sicrhau parhad prosesau a gweithrediadau'r busnes os amharir ar y gwasanaeth neu os yw'n methu ac ar gyfer adfer y gwasanaeth drwy gyfrwng gweithdrefnau parhad busnes ac, fel y bo angen, weithdrefnau adfer ar ôl trychineb. Mae hefyd yn cynnwys y gofyn ar y contractwr i ddatblygu, adolygu, profi, newid a chynnal Cynllun BCDR ar gyfer y gwasanaeth.

Atodlen 4.2 Gwybodaeth Fasnachol Sensitif (Llywodraethu Gwybodaeth)

Bwriedir yr atodlen hon i nodi'r agweddau ar y cytundeb y mae'r contractwr yn ystyried eu bod yn 'fasnachol sensitif', ac felly y byddai eu datgelu yn andwyol i'w busnes a/neu fudd y cyhoedd. Os ceir cais Rhyddid Gwybodaeth, byddai'r awdurdod yn ystyried hwn ond ni fyddai ynddo'i hun yn atal yr awdurdod rhag datgelu'r wybodaeth os oedd yn ofynnol iddo wneud hynny.

Atodlen 7.2 Archwiliadau a Gwerth am Arian (Llywodraethu Gwybodaeth a Diogelwch)
Yn ogystal â chaniatáu i GIG Cymru feincnodi taliadau yn y cytundeb hwn, mae'r contract hwn yn caniatáu ac yn galluogi'r awdurdod i gael mynediad i'r wybodaeth sy'n ofynnol i fodloni ei ofynion archwilio ei hun h.y. Archwiliadau Diogelwch a Llywodraethu Gwybodaeth.

Atodlen 8.5 Trefniadau Ymadael (Diogelwch)
Yn datgan egwyddorion y trefniadau ymadael a throsglwyddo gwasanaethau y'u bwriedir er mwyn sicrhau trosglwyddo trefnus ar ddiwedd y cytundeb hwn, megis trosglwyddo data.

Telerau ac Amodau Syml (SIMCON yn flaenorol)

Cytundeb Atebion a Gwasanaethau TG syml ar gyfer atebion sy'n llai cymhleth ac sydd â gwerth is h.y. dan £10m.

Telerau Contractiol Allweddol Llywodraethu Gwybodaeth
Yn diffinio'r Prosesydd Data a'r Rheolydd Data – y Contractwr yw'r Prosesydd Data a'r Awdurdod yw'r Rheolydd Data.

Yn caniatáu i'r contractwr brosesu data o safbwynt cyflenwi'r cytundeb yn unol â'r Ddeddf Diogelu Data, y rhwymedigaethau sy'n cael eu datgan dan y cytundeb ac unrhyw gyfarwyddiadau gan yr awdurdod o bryd i'w gilydd.

Yn datgan eu rhwymedigaethau o safbwynt y canlynol:

- Cydymffurfio â'r Ddeddf Diogelu Data;
- Delio'n brydlon ag ymholiadau'r Comisiynydd Gwybodaeth a'r Awdurdod am brosesu data;
- Ceisiadau oddi wrth unigolion ynglŷn â gweld eu data personol;
- Datgelu neu fynediad i gofnodion anawdurdodedig;
- Dim ond datgelu data wrth bersonél awdurdodedig i gyflenwi'r contract;
- Mesurau diogelwch technegol a threfniadol i fod ar waith gan y contractwr i sicrhau na cheir mynediad heb ei awdurdodi i ddata ac na chaiff ei brosesu'n anghyfreithlon;
- Sicrhau nad yw gweithredoedd y contractwr yn gwneud dim a fyddai'n achosi i'r Data gael ei drosglwyddo y tu allan i Ardal Economaidd Ewrop;
- Y contractwr sy'n gyfrifol am dalu unrhyw gostau o safbwynt unrhyw ddiweddariad i'r Ddeddf Diogelu Data i sicrhau eu bod yn cydymffurfio;
- Sicrhau eu bod yn cadw data yn gyfrinachol oni roddir caniatâd penodol i ddatgelu;
- Terfynu; ar y dyddiad y daw'r Cytundeb i ben neu ynghynt, rhaid i'r Contractwr sicrhau bod yr holl ddogfennau/cofnodion sydd yn nwylo neu dan reolaeth y contractwr yn cael eu dileu'n barhaol;
- Ar ôl terfynu'r contract, rhaid i'r Contractwr beidio â defnyddio Data'r Awdurdod; ac
- Bod darpariaethau ar gyfer archwiliadau data gan yr Awdurdod yn y Cytundeb.

FOIA

- Defnyddio rhannu data a rhwymedigaethau i lynu wrthynt o safbwynt rhannu data a'r Ddeddf Rhyddid Gwybodaeth.

Telerau Contractiol Allweddol Diogelwch

- Personél y Contractwr yn cydymffurfio â'r Cynllun a'r Gofynion Diogelwch a'r Polisi Diogelwch;
- Bydd y Contractwr yn glynu wrth ofynion Diogelwch GIG Cymru gan gynnwys cynnal profion hacio ar yr ateb pan gaiff ei weithredu yn gyntaf

ac yn flynyddol drwy gyfrwng Ymgynghorydd CLAS ac yn glynu wrth Safonau CHECK;

- Bod darpariaethau ar gyfer archwiliadau diogelwch o'r ateb gan yr Awdurdod yn y Cytundeb;
- Defnyddio patsys diogelwch a glynu wrth Bolisi Diogelwch yr Awdurdod;
- Rhaid i'r holl Weinyddwyr a ddefnyddir dan y contract gael eu caledu;
- Cynnal cynllun i ddelio â digwyddiad seiberddiogelwch; a
- Dim data i adael rhwydwaith GIG Cymru heb ganiatâd ysgrifenedig.