Arolygiaeth Ei Mawrhydi dros Addysg a Hyfforddiant yng Nghymru
Her Majesty's Inspectorate for Education and Training in Wales

Polisi diogelu gwybodaeth

Taflen wybodaeth

Blwch gwybodaeth I gael cyngor pellach, cysylltwch â'r: Grŵp Rheoli Gwybodaeth Dyddiad cyhoeddi: Gorffennaf 2021 Fersiwn: 1.0

Rheoli fersiwn

Fersiwn o'r ddogfen	Awdur	Dyddiad cyhoeddi	Newidiadau a wnaed
1.0	Phil Sweeney	Gorffennaf 2021	

Asesiad o Effaith ar Gydraddoldeb

Cynhaliwyd asesiad o resymwaith busnes ac mae'r polisi hwn yn cyfrannu at amcanion strategol ac egwyddorion cyflawni Estyn.

Yn unol ag Asesiad Estyn o Effaith ar Gydraddoldeb, cynhaliwyd asesiad cychwynnol o effaith sgrinio ac ystyrir nad yw'r polisi hwn yn cael effaith niweidiol ar sail y naw nodwedd warchodedig fel a nodir yn Neddf Cydraddoldeb 2010.

Cynnwys	Tudalen

1 Cyflwyniad 1

1.1 Cefndir 1
1.2 Nodau 1
1.3 Amcanion 2
1.4 Cwmpas 2

2 Rolau a chyfrifoldebau 2

2.1 Prif Arolygydd Ei Mawrhydi (PAEM) 2
2.2 Uwch Berchennog Risg Gwybodaeth 2
2.3 Swyddog Diogelu Data (SDD) 2
2.4 Perchnogion Asedau Gwybodaeth (PAG) 3
2.5 Cadeirydd y Grŵp Rheoli Gwybodaeth (GRhG) 3
2.6 Swyddog Diogelu Seiberddiogelwch TG 3
2.7 Pob aelod o staff 3

3 Fframwaith polisi 4

3.1 Contractau cyflogaeth 4
3.2 Rheoli diogelwch asedau 4
3.3 Rheolaethau mynediad 4
3.4 Gweithdrefnau cyfrifiadur a rhwydwaith 5
3.5 Asesu risg gwybodaeth 5
3.6 Digwyddiadau a gwendidau diogelu gwybodaeth 5
3.7 Dosbarthu gwybodaeth sensitif 5
3.8 Diogelu rhag meddalwedd faleisus 5
3.9 Mynediad at system fonitro a'i defnyddio 5
3.10 Rheoli newid systemau 6
3.11 Achredu systemau gwybodaeth 6
3.12 Parhad busnes a chynlluniau adfer rhag trychineb 6
3.13 Hyfforddiant ac ymwybyddiaeth 6

4 Monitro 7

1 Cyflwyniad

1.1 Cefndir

Mae Estyn yn gorff cyhoeddus sydd â phrosesu gwybodaeth yn rhan sylfaenol o'i ddiben. Felly, mae'n bwysig bod gennym ni Bolisi Diogelu Gwybodaeth clir a pherthnasol. Mae hyn yn hanfodol wrth i ni gydymffurfio â deddfwriaeth diogelu data a deddfwriaeth arall, a sicrhau bod cyfrinachedd yn cael ei barchu.

Mae'r ddogfen hon yn amlinellu'r polisi a'r gweithdrefnau lefel uchel i ddiogelu ein holl asedau gwybodaeth i safon gyson uchel. Mae'r polisi'n cwmpasu diogelwch y gellir ei gymhwyso trwy dechnoleg a rheolaethau prosesau, ond efallai mai'r hyn sy'n fwy tyngedfennol yw ei fod yn cwmpasu cyfrifoldebau ac ymddygiad y bobl sy'n rheoli gwybodaeth yn unol â'n busnes.

Mae diogelu gwybodaeth ynglyn ag ymddygiad pobl o ran y wybodaeth y maent yn gyfrifol amdani, wedi'i hwyluso gan ddefnyddio technoleg yn briodol. Dyma fanteision busnes y polisi hwn a'r arweiniad cysylltiedig:

- Sicrhau bod gwybodaeth yn cael ei rheoli'n ddiogel ac mewn ffordd gyson a chorfforaethol.
- Sicrhau ein bod yn gweithredu amgylchedd diogel yr ymddiriedir ynddo ar gyfer rheoli'r wybodaeth a ddefnyddir wrth gyflawni ein busnes.
- Eglurder ynghylch y cyfrifoldebau personol yn gysylltiedig â diogelu gwybodaeth a ddisgwylir o staff wrth iddynt weithio i ni.
- Sefyllfa gryfach os caiff unrhyw gamau cyfreithiol eu cymryd yn ein herbyn ni (gan dybio y caiff y polisi ei gymhwyso'n briodol, a chydymffurfiad priodol ag ef).
- Arddangos arfer orau wrth ddiogelu gwybodaeth.
- Sicrhau bod gwybodaeth ar gael dim ond i'r rhai sydd ag awdurdod i allu cael y wybodaeth.
- Sicrhau bod risgiau'n cael eu nodi a bod rheolaethau priodol yn cael eu gweithredu a'u dogfennu.

1.2 Nod

Nod y polisi hwn yw gwarchod:

Cyfrinachedd	Dylid cyfyngu mynediad at ddata i'r rhai sydd ag awdurdod priodol.
Uniondeb	Dylai gwybodaeth fod yn gyflawn a chywir. Dylai'r holl systemau, asedau a rhwydweithiau weithredu'n gywir, yn unol â'r fanyleb.
Argaeledd	Dylid trefnu bod gwybodaeth ar gael a'i danfon at yr unigolyn cywir, pan fydd ei hangen.

1.3 Amcanion

Amcanion y polisi hwn yw sefydlu a chynnal diogelwch a chyfrinachedd ein gwybodaeth, systemau gwybodaeth, cymwysiadau a rhwydweithiau trwy:

- Sicrhau bod pob aelod o staff yn ymwybodol o'u rolau, cyfrifoldebau ac atebolrwydd ac yn cydymffurfio'n llawn â'r ddeddfwriaeth berthnasol fel y disgrifir yn y polisi hwn, ac mewn polisïau eraill Rheoli Gwybodaeth
- Disgrifio egwyddorion diogelu ac esbonio sut cânt eu rhoi ar waith yn y sefydliad. Cyflwyno ymagwedd gyson at ddiogelwch, gan sicrhau bod pob aelod o staff yn deall eu cyfrifoldebau eu hunain yn llawn
- Creu a chynnal lefel o ymwybyddiaeth o'r angen am Ddiogelu Gwybodaeth fel rhan annatod o'n busnes o ddydd i ddydd
- Diogelu asedau gwybodaeth o dan ein rheolaeth

1.4 Cwmpas

Mae staff sy'n gweithio yn Estyn, neu ar ein rhan (mae hyn yn cynnwys contractwyr, staff dros dro, staff ar secondiad / ar fenthyg a'r holl gyflogeion parhaol) o fewn cwmpas y polisi hwn.

2 Rolau a chyfrifoldebau

2.1 Prif Arolygydd Ei Mawrhydi (PAEM)

Mae cyfrifoldeb am ddiogelu gwybodaeth yn aros gyda PAEM, yn y pen draw. Cyflawnir y cyfrifoldeb hwn trwy rolau dynodedig Uwch Berchennog Risg Gwybodaeth.

2.2 Uwch Berchennog Risg Gwybodaeth

Mae'r Uwch Berchennog Risg Gwybodaeth yn gyfrifol am risg gwybodaeth yn Estyn, ac yn cynghori'r Bwrdd Gweithredol a'r Bwrdd Strategaeth ar effeithiolrwydd ein rheolaeth risg gwybodaeth. Mae'r rôl hon wedi'i dynodi i'r Cyfarwyddwr Gwasanaethau Corfforaethol (Phil Sweeney) ar hyn o bryd.

2.3 Swyddog Diogelu Data (SDD)

A ninnau'n awdurdod cyhoeddus, mae'n ofynnol i ni benodi Swyddog Diogelu Data yn ôl y Rheoliad Cyffredinol ar Ddiogelu Data (GDPR). Mae'r SDD yn gyfrifol am ddarparu cyngor, monitro cydymffurfio, a dyma'r unigolyn cyswllt cyntaf yn y sefydliad ar gyfer materion diogelu data. Mae'r SDD yn adrodd i'r Uwch Berchennog Risg Gwybodaeth o ran materion diogelu data.

2.4 Perchnogion Asedau Gwybodaeth

Mae Perchnogion Asedau Gwybodaeth yn gyfrifol am ddiogelwch eu hamgylchoedd (ffisegol a digidol) lle caiff gwybodaeth ei phrosesu neu'i storio. Hefyd, maent yn gyfrifol, ar y cyd â rheolwyr, am y canlynol:

- Sicrhau bod pob aelod o staff, parhaol, dros dro a chontractwr, yn ymwybodol o'r polisïau a'r gweithdrefnau diogelu gwybodaeth, a rhwymedigaethau defnyddwyr sy'n berthnasol i'w maes gwaith i gynnal diogelwch da o ran gwybodaeth
- Pennu'r lefel mynediad y dylid ei rhoi i unigolion penodol
- Sicrhau bod staff yn cael hyfforddiant priodol ar gyfer y systemau y maent yn eu defnyddio
- Sicrhau bod staff yn gwybod sut i gael cyngor ar faterion diogelu gwybodaeth

Mae pob Perchennog Asedau Gwybodaeth yn gyfrifol am sicrhau bod proseswyr data trydydd parti yn cael achrediad priodol ISO a/ neu achrediad Cyber Essentials lle bo'n briodol ar gyfer asedau sy'n cael eu storio'n electronig gyda thrydydd partïon. Hefyd, mae Perchnogion Asedau Gwybodaeth yn gyfrifol am sicrwydd diogelu data priodol gan bob cyflenwr trydydd parti sy'n prosesu ein data.

2.5 Cadeirydd y Grŵp Rheoli Gwybodaeth

Bydd Cadeirydd y Grŵp Rheoli Gwybodaeth yn gyfrifol am gynnal polisïau ac arweiniad priodol ar gyfer staff ynglŷn â defnyddio a phrosesu data personol gwybodaeth sydd wedi'i chynnwys o fewn ein hasedau gwybodaeth, yn unol â deddfwriaeth a rheoliadau gwarchod a diogelu data.

2.6 Swyddog Seiberddiogelwch TG

Caiff rôl Cadeirydd y Grŵp Rheoli Gwybodaeth ei chefnogi gan y Swyddog Seiberddiogelwch TG.

Mae'r Swyddog Seiberddiogelwch TG yn gyfrifol am ddatblygu, gweithredu a grymuso gweithdrefnau a phrotocolau addas a pherthnasol ar gyfer diogelu gwybodaeth i sicrhau bod mesurau digonol gan ein systemau, offer a seilwaith i gydymffurfio â deddfwriaeth a rheoliadau gwarchod a diogelu data.

2.7 Pob aelod o staff

Mae pob aelod o staff yn gyfrifol am ddiogelwch gwybodaeth y data y maent yn ei ddefnyddio neu'n cael mynediad ato yn sgil eu cyflogaeth gydag Estyn, ac felly rhaid iddynt ddeall y polisi hwn ac arweiniad cysylltiedig, a chydymffurfio â nhw. Gallai methiant i wneud hynny arwain at gamau disgyblu. Yn benodol, dylai pob aelod o staff ymgymryd â hyfforddiant Ymwybyddiaeth Diogelu Gwybodaeth, a deall:

- Pa wybodaeth y maent yn ei defnyddio, sut dylid ei thrin, ei storio a'i throsglwyddo yn ddiogel
- Pa weithdrefnau, safonau a phrotocolau sy'n bodoli ar gyfer rhannu gwybodaeth gydag eraill
- Sut i adrodd am achos a amheuir o dorri rheolau diogelu gwybodaeth yn Estyn

- Eu cyfrifoldeb i godi unrhyw bryderon am ddiogelu gwybodaeth gyda'r Swyddog Seiberddiogelwch TG

3 Fframwaith polisi

3.1 Contractau cyflogaeth

Dylid mynd i'r afael â gofynion diogelu staff yn y cam recriwtio, a dylai pob contract cyflogaeth gynnwys cymal priodol ar gyfrinachedd.

Dylid cwmpasu disgwyliadau diogelu gwybodaeth o ran staff yn y broses ymsefydlu, a chyfeirio atynt mewn diffiniadau a disgrifiadau priodol o swyddi.

3.2 Rheoli diogelwch asedau

Bydd y tîm Gwasanaethau Swyddfa yn sefydlu ac yn cynnal proses rheoli asedau TG a system gysylltiedig; dylai fod Perchennog Asedau Gwybodaeth enwebedig ar gyfer yr holl asedau TG, (caledwedd, meddalwedd, cymhwysiad neu ddata) a fydd yn gyfrifol am ddiogelu gwybodaeth yr ased hwnnw.

Er mwyn lleihau colli neu ddifrodi'r holl asedau, dylai'r tîm Gwasanaethau Swyddfa sicrhau bod yr holl offer ac asedau electronig yn cael eu nodi, eu cofrestru a'u diogelu'n ffisegol rhag bygythiadau a pheryglon amgylcheddol.

3.3 Rheolaethau mynediad

Dylid cyfyngu mynediad at wybodaeth i ddefnyddwyr sydd ag angen busnes awdurdodedig i fynd at y wybodaeth, a dylai gyd-fynd â chymeradwyaeth gan y Perchennog Asedau Gwybodaeth perthnasol.

Rhaid i berchnogion systemau sicrhau bod rheolaethau mynediad yn cael eu cynnal ar lefelau priodol a bod unrhyw newidiadau i ganiatâd mynediad wedi eu hawdurdodi. Rhaid cynnal cofnod o'r caniatâd mynediad a roddwyd. Rhaid i fynediad at yr holl Systemau TG ddefnyddio proses fewngofnodi ddiogel a gallai mynediad gael ei gyfyngu gan adeg y dydd neu gan leoliad y derfynell gychwynnol, neu'r naill a'r llall.

Rhaid i reolwyr llinell sicrhau bod mynediad at systemau TG ar gael i gyflogeion yn ystod cyfnod eu cyflogaeth yn unig. Yn benodol, rhaid i reolwyr llinell sicrhau bod mynediad ymadawyr at systemau yn cael ei dynnu'n ôl cyn gynted ag y caiff cyflogaeth ei therfynu; bydd y tîm AD yn cynnal rhestr wirio o achosion o dynnu mynediad at systemau.

Dylai mynediad at ddata, cyfleustodau system a llyfrgelloedd ffynonellau rhaglen gael eu rheoli a'u cyfyngu i'r defnyddwyr awdurdodedig hynny sydd ag angen busnes dilys, e.e. gweinyddwyr systemau neu gronfeydd data. Bydd awdurdod i ddefnyddio cymhwysiad yn dibynnu ar argaeledd trwydded gan y cyflenwr.

Rhaid i gontractau â chontractwyr allanol sy'n caniatáu mynediad at ein systemau gwybodaeth fod yn weithredol cyn caniatáu mynediad. Rhaid i'r contractau hyn

sicrhau bod staff neu is-gontractwyr y sefydliad allanol yn cydymffurfio â'r holl bolisïau diogelu priodol.

3.4 Gweithdrefnau cyfrifiadur a rhwydwaith

Dylai cyfrifiaduron a rhwydweithiau gael eu rheoli trwy weithdrefnau safonol wedi eu dogfennu. Hefyd, bydd angen systemau a phrosesau cytûn ar gyfer hyn lle bydd cymorth TG yn cael ei ddarparu gan ffynonellau allanol, a gwerthwyr trydydd parti yn gweithio i Estyn, ac ar ei ran.

3.5 Asesu risg gwybodaeth

Bydd yr holl asedau gwybodaeth yn cael eu nodi a Pherchennog Asedau Gwybodaeth yn cael eu dynodi ar eu cyfer. Dylai Perchnogion Asedau Gwybodaeth sicrhau bod asesiadau risg gwybodaeth yn cael eu cynnal bob blwyddyn, o leiaf, gan ddilyn arweiniad gan yr Uwch Berchennog Risg Gwybodaeth. Bydd Perchnogion Asedau Gwybodaeth yn cyflwyno canlyniadau'r asesiad risg a chynlluniau lliniaru cysylltiedig i'w hadolygu yng nghyfarfodydd y Grŵp Rheoli Gwybodaeth. Bydd y Grŵp Rheoli Gwybodaeth yn cynnal ac yn adolygu Cofrestr Risg Gwybodaeth drosfwaol.

3.6 Digwyddiadau a gwendidau diogelu gwybodaeth

Dylid rhoi gwybod i'r Uwch Berchennog Risg Gwybodaeth a'r Swyddog Seiberddiogelwch TG am yr holl ddigwyddiadau diogelu gwybodaeth, achosion y bu bron iddynt ddigwydd ac amheuon o wendidau. Rhaid cydymffurfio â'r gweithdrefnau Adrodd am Achosion Diogelu Gwybodaeth.

3.7 Dosbarthu gwybodaeth sensitif

Byddwn yn gweithredu rheolaethau dosbarthiadau gwybodaeth priodol, wedi eu seilio ar ganlyniadau asesu risg ac arweiniad ffurfiol sydd wedi eu cynnwys yn y Polisi Sicrhau Gwybodaeth a chyfarwyddiadau desg perthnasol.

3.8 Diogelu rhag meddalwedd faleisus

Byddwn yn gweithio gyda darparwyr gwasanaeth TG i ddefnyddio gwrth-fesurau a gweithdrefnau rheoli meddalwedd i amddiffyn yn erbyn bygythiad meddalwedd faleisus. Bydd disgwyl i bob aelod o staff gydweithredu'n llawn â'r Polisi Defnyddio TG, e.e. ni ddylai unigolion osod meddalwedd heb y caniatâd priodol.

3.9 Mynediad at system fonitro a'i defnyddio

Dylid cynnal ac adolygu trywydd archwilio mynediad at systemau a defnydd staff o ddata yn rheolaidd i gefnogi gwiriadau cydymffurfio â'r polisi hwn a pholisïau eraill, a monitro gweithgarwch lle amheuir bod y polisi wedi cael ei dorri, os oes angen. Mae Deddf Rheoleiddio Pwerau Ymchwilio (2000) yn caniatáu monitro a chofnodi cyfathrebu electronig cyflogeion (yn cynnwys cyfathrebu dros y ffôn) am y rhesymau canlynol:

- Sefydlu bodolaeth ffeithiau
- Ymchwilio i, neu ganfod, defnydd anawdurdodedig o'r system
- Atal neu ganfod troseddau
- Canfod neu ddangos safonau a gyflawnir neu y dylid eu cyflawni gan bobl sy'n defnyddio'r system (rheoli ansawdd a hyfforddiant)
- Er budd diogelwch gwladol
- Canfod a oes cydymffurfiaeth ag arferion neu weithdrefnau rheoleiddio neu hunanreoleiddio
- Sicrhau bod y system yn gweithredu'n effeithiol.

Bydd unrhyw fonitro yn cael ei wneud yn unol â'r Ddeddf uchod a'r Ddeddf Hawliau Dynol, ac unrhyw gyfraith arall berthnasol.

3.10 Rheoli newid systemau

Bydd newidiadau i systemau gwybodaeth, cymwysiadau neu rwydweithiau yn cael eu hadolygu a'u cymeradwyo gan y Swyddog Seiberddiogelwch TG ar y cyd â Pherchennog y System. Rhaid i Berchnogion Systemau sicrhau bod caffael neu weithredu meddalwedd newydd neu wedi'i huwchraddio yn cael ei gynllunio a'i reoli'n ofalus, a bod unrhyw ddatblygiad ar gyfer Estyn, neu ganddo, bob amser yn dilyn proses ddatblygu ffurfiol gyda thrywyddau archwilio priodol. Rhaid lliniaru risgiau diogelu gwybodaeth gyda phrosiectau o'r fath gan ddefnyddio cyfuniad o reolaethau gweithdrefnol a thechnegol. Rhaid i ofynion busnes ar gyfer meddalwedd newydd neu wella meddalwedd bresennol nodi'r gofynion ar gyfer rheolaethau diogelu gwybodaeth.

3.11 Achredu systemau gwybodaeth

Byddwn yn sicrhau bod yr holl systemau gwybodaeth, cymwysiadau a rhwydweithiau newydd yn cynnwys Polisi Diogelu Lefel System (SLSP) ac yn cael eu cymeradwyo gan y Swyddog Seiberddiogelwch TG cyn iddynt ddechrau gweithredu. Bydd Perchennog System dynodedig i bob system. Rhaid i'r Uwch Berchennog Risg Gwybodaeth gymeradwyo:

- Unrhyw broses newydd sy'n cynnwys prosesu data personol (data yn ymwneud ag unigolion)
- Newidiadau i'w gwneud i broses bresennol sy'n cynnwys prosesu data personol
- Caffael system wybodaeth newydd sy'n prosesu data personol, neu drwyddedu system trydydd parti sy'n cynnal ac / neu'n prosesu data personol
- Unrhyw dechnoleg newydd sy'n defnyddio neu'n prosesu data personol mewn unrhyw ffordd

3.12 Parhad busnes a chynlluniau adfer rhag trychineb

Bydd cynlluniau parhad busnes yn cael eu rhoi ar waith gan Berchnogion Systemau i sicrhau parhad gweithgareddau wedi eu blaenoriaethu mewn digwyddiad sylweddol neu fawr.

Bydd yr Uwch Berchennog Risg Gwybodaeth yn ceisio cael sicrwydd gan Berchnogion Systemau fod cynlluniau priodol adfer rhag trychineb ar waith ar gyfer

yr holl gymwysiadau, systemau a rhwydweithiau blaenoriaeth, a bod y cynlluniau hyn yn cael eu hadolygu a'u profi'n rheolaidd i ddarparu tystiolaeth fod prosesau adnewyddu ac adfer wrth gefn yn effeithiol.

3.13 Hyfforddiant ac ymwybyddiaeth

Mae hyfforddiant diogelu gwybodaeth yn orfodol ac mae'n ofynnol i bob aelod o staff gwblhau hyfforddiant ar-lein yn unol â chyfnodau amserlenedig. Mae'n ofynnol i bob aelod o staff gadarnhau eu bod wedi darllen polisïau perthnasol wedi eu dynodi o fewn ein fframwaith rheoli gwybodaeth – bydd diweddariadau rheolaidd yn gysylltiedig â materion rheoli a diogelu yn cael eu darparu, ynghyd â gwiriadau ar ymwybyddiaeth ynghylch materion a risgiau fel ceisio gwe-rwydo a risgiau meddalwedd wystlo.

4 Monitro

Bydd cydymffurfio â'r polisïau a'r gweithdrefnau a nodir yn y ddogfen hon yn cael ei fonitro trwy'r Grŵp Rheoli Gwybodaeth, ynghyd ag adolygiadau archwilio annibynnol o bryd i'w gilydd. Bydd y Grŵp Rheoli Gwybodaeth yn gyfrifol am ddiweddaru'r ddogfen hon a pholisïau ac arweiniad cysylltiedig hefyd, ac am nodi anghenion hyfforddi staff parhaus a rhai sy'n dod i'r amlwg.