Cyngor Sir Caerfyrddin

Polisi Diogelwch Gwybodaeth

Cynnwys

1. Rhagarweiniad

1.1 Mae rheoli diogelwch gwybodaeth yn galluogi'r wybodaeth i gael ei rhannu, gan sicrhau diogelwch y wybodaeth a'r asedau caledwedd ar yr un pryd. Mae tair elfen sylfaenol:

- **Cyfrinachedd:** diogelu gwybodaeth sensitif rhag cael ei rhyng-gipio neu ei datgelu heb awdurdod
- **Uniondeb:** diogelu cywirdeb y wybodaeth
- **Argaeledd:** sicrhau bod gwybodaeth ar gael i aelodau, gweithwyr, cyrff allanol a'r cyhoedd pan fydd angen

1.2 Prif amcanion y polisi yw sicrhau:

- Bod asedau gwybodaeth ac offer TGCh y Cyngor yn cael eu diogelu'n ddigonol rhag unrhyw gamau a allai gael effaith andwyol ar ddiogelwch gwybodaeth.
- Bod yn rhaid i bob ased gwybodaeth fod yn "eiddo" i swyddog penodol yn yr awdurdod. Bod y Cyngor yn diffinio pob Pennaeth Gwasanaeth fel **Perchennog Asedau Gwybodaeth.**
- Bod y staff ac aelodau etholedig yn gwybod am yr holl ddeddfwriaeth berthnasol a pholisïau'r Cyngor ac yn cydymffurfio â hwy wrth gyflawni eu dyletswyddau beunyddiol o ran TGCh.

2. Cwmpas

2.1 Mae'r polisi hwn yn berthnasol i'r holl asedau gwybodaeth a ddelir gan Gyngor Sir Caerfyrddin. Diffinnir ased gwybodaeth fel:

> *"ased electronig neu ased nad yw'n electronig, sy'n eiddo i'r Cyngor neu a ymddiriedwyd iddo (gan gwsmeriaid mewnol ac allanol) ac sy'n cynnwys, ond heb fod yn gyfyngedig i, bob dogfen ar ffurf copi caled a data electronig a gedwir yn ein systemau a'n cronfeydd data."*

2.2 Mae'r polisi hwn yn berthnasol i:

- Holl weithwyr ac aelodau etholedig y Cyngor
- Holl weithwyr ac asiantiaid sefydliadau eraill sy'n cefnogi neu'n defnyddio rhwydwaith y Cyngor yn uniongyrchol neu'n anuniongyrchol
- Holl staff dros dro a gyflogir yn uniongyrchol neu'n anuniongyrchol gan y Cyngor

- Holl bobl sy'n gwneud gwaith ar ran y Cyngor ar sail wirfoddol
- Holl ddefnyddwyr sy'n defnyddio systemau, rhwydweithiau ac adnoddau TG sy'n eiddo i'r Cyngor

3. Datganiadau Polisi

3.1 Bydd y Cyngor yn gweithredu rheolaethau ac arferion i gefnogi cysyniadau craidd Cyfrinachedd, Uniondeb ac Argaeledd er mwyn atal asedau gwybodaeth rhag cael eu colli neu eu llygru ac er mwyn lleihau'r risg na fydd gwybodaeth ar gael i'r defnyddiwr.

3.1 Defnyddir asedau gwybodaeth y Cyngor yn unol â'r canlynol:

- Y Polisi Diogelwch Gwybodaeth hwn
- Y Polisi a'r Weithdrefn ar gyfer Trin Gwybodaeth Bersonol
- Polisi Riportio ac Ymateb i Achosion o Dorri Rheolau
- Polisi Defnyddio'r E-bost a Monitro Hynny
- Polisi Defnyddio'r Rhyngrwyd a Monitro Hynny
- Deddfwriaeth berthnasol - gan gynnwys (ond heb fod yn gyfyngedig iddynt) y Rheoliad Diogelu Data Cyffredinol, Deddf Diogelu Data 2018, Deddf Camddefnyddio Cyfrifiaduron 1990, Deddf Rhyddid Gwybodaeth 2000 a'r Ddeddf Hawlfreintiau, Dyluniadau a Phatentau

3.2 Gellir cymryd camau disgyblu yn erbyn unrhyw un nad yw'n cydymffurfio â'r polisi hwn.

3.3 Mae'r polisi hwn wedi'i gymeradwyo gan y Cyngor ac mae'n cael ei gefnogi'n llwyr ganddo.

4. Cyfrifoldebau

4.1 Mae pob aelod o staff yn gyfrifol am:

- Helpu i ddiogelu systemau ac offer y Cyngor drwy gydymffurfio â'r gofynion diogelwch a geir yn y ddogfen hon.
- Defnyddio'r holl fesurau a dulliau diogelwch priodol i warchod rhaglenni a ffeiliau data a gwneud yn siŵr bod gwybodaeth bersonol neu gyfrinachol, boed yn electronig neu ar bapur, yn ddiogel rhag achosion o ddwyn, rhag cael ei datgelu/defnyddio heb ganiatâd, rhag cael ei cholli drwy ddamwain a'i difa.
- Peidio â cheisio tanseilio neu osgoi unrhyw ddulliau diogelwch a osodwyd. Mae hyn yn cynnwys peidio â rhannu cyfrineiriau; ni ddylai defnyddwyr byth, o dan unrhyw amgylchiadau, ddatgelu eu cyfrineiriau i

neb na chaniatáu i ddefnyddiwr arall rannu eu manylion er mwyn goresgyn rheolaethau mynediad.

- Dilyn **Polisi Riportio ac Ymateb i Achosion o Dorri Rheolau** y Cyngor pan fydd amheuaeth bod achos o dorri rheolau data personol wedi digwydd.
- Os amheuir defnydd heb ganiatâd o offer y Cyngor, feirws cyfrifiadurol neu ymosodiad seibr, tynnwch y mater at sylw'r Ddesg Gymorth TG yn ddi-oed.
- Sicrhau bod holl ddata'r Cyngor yn cael ei storio ar system fusnes neu gynllun ffeiliau'r Cyngor ac nid ar yriant caled y cyfrifiadur.
- Sicrhau bod dyfeisiau cludadwy a chyfryngau symudadwy wedi'u hamgryptio a dim ond yn cael eu defnyddio mewn amgylchiadau eithriadol ac yn unol â'r **Polisi Defnyddio Dyfeisiau Cludadwy** a'r **Polisi Trin Gwybodaeth Bersonol**.
- Sicrhau mai dim ond meddalwedd a awdurdodwyd sy'n cael ei roi ar systemau'r Cyngor.
- Defnyddio dyfeisiau a awdurdodwyd yn unig ar rwydwaith corfforaethol y Cyngor.
- Sicrhau bod offer TGCh dim ond yn cael ei waredu mewn modd diogel sydd wedi'i drefnu gan y Gwasanaethau TGCh.
- Sicrhau bod system e-bost y Cyngor yn cael ei defnyddio yn unol â **Pholisi Defnyddio'r E-bost a Monitro Hynny.**
- Sicrhau bod unrhyw fynediad i'r rhyngrwyd yn unol â **Pholisi Defnyddio'r Rhyngrwyd a Monitro Hynny y Cyngor.**
- Sicrhau yr ymdrinnir â data personol yn unol â **Pholisi a Gweithdrefn y Cyngor ynghylch Trin Gwybodaeth Bersonol.**
- Sicrhau eu bod yn gwybod am yr holl Bolisïau Llywodraethu Gwybodaeth a chanllawiau cysylltiedig ac yn eu deall.

4.2 Mae Rheolwyr Llinell yn gyfrifol am:

- Sicrhau bod eu gweithwyr yn gwybod am yr holl ofynion diogelwch sy'n ymwneud ag offer, cyfleusterau a data TGCh ac yn cydymffurfio â nhw.
- Sicrhau bod eu gweithwyr yn ymwybodol o'r holl ofynion cyfreithiol sy'n ymwneud â defnyddio meddalwedd perchnogol ac yn cydymffurfio â nhw, e.e. parchu hawlfreintiau a thrwyddedau safle.
- Sicrhau bod gweithwyr y maent yn gyfrifol amdanynt yn cael hyfforddiant priodol mewn ymwybyddiaeth o ddiogelwch, gan gynnwys deunydd ar gyfer gofynion cyfreithiol megis y Rheoliad Diogelu Data Cyffredinol (GDPR). Rhaid i bob rheolwr llinell drefnu hyfforddiant i bob gweithiwr newydd a hyfforddiant achlysurol i'r holl staff, i ymateb i newidiadau mewn gweithdrefnau a deddfwriaeth.
- Sicrhau bod hawliau mynediad gweithwyr sy'n ymadael â'r awdurdod neu sy'n trosglwyddo i adran arall yn cael eu hadolygu a'u diddymu lle bo hynny'n briodol, a bod offer TGCh yn cael ei ddychwelyd

4.3 Mae Penaethiaid Gwasanaeth, fel Perchnogion Asedau Gwybodaeth, yn gyfrifol am:

- Diogelwch gwybodaeth yn gyffredinol yn eu maes gwasanaeth.
- Darparu cymorth ac adnoddau rheoli i gyflawni gofynion y polisi hwn.
- Sicrhau bod yr holl brif raglenni ac adnoddau wedi'u clustnodi a bod "Perchennog System" wedi'i benodi ar gyfer pob prif raglen/system. Sicrhau y cydymffurfir â'r holl ofynion cyfreithiol sy'n ymwneud â defnyddio meddalwedd perchnogol masnachol e.e. parchu hawlfreintiau a thrwyddedau safle.
- Mynd i'r afael â diogelwch wrth recriwtio, gan sicrhau bod gofynion diogelwch yn cael eu cynnwys mewn disgrifiadau swyddi a chontractau cyflogaeth.
- Sicrhau bod darpar weithwyr yn cael eu sgrinio'n briodol, yn enwedig ar gyfer swyddi mewn meysydd sensitif megis gofal cymdeithasol.
- Sicrhau bod gweithwyr a thrydydd partïon yn gwybod mai eiddo'r Cyngor yw'r wybodaeth ac y dylid ei drin yn gyfrinachol, gan y gallai datgelu gwybodaeth heb ganiatâd arwain at gamau disgyblu, neu, yn achos trydydd partïon, at golli contractau neu berthynas waith.
- Sicrhau bod defnyddwyr yn cael caniatâd ysgrifenedig yn disgrifio'u hawliau mynediad a'r cyfyngiadau ar yr hawliau hynny. Er enghraifft, i ganiatáu mynediad i wybodaeth na cheir caniatâd iddi fel arall.
- Rhoi adnoddau a chyngor i'r Gwasanaethau TGCh wrth ymateb i achos o dorri rheolau data personol neu ddigwyddiad diogelwch.
- Paratoi cynlluniau parhad busnes i ddiogelu prosesau busnes hollbwysig rhag effeithiau methiannau mawr neu argyfyngau. Caiff gweithdrefnau eu rhoi ar waith i ddatblygu a chynnal cynlluniau priodol ar gyfer adfer prosesau busnes a gwasanaethau hollbwysig yn gyflym os digwydd rhywbeth sy'n amharu'n ddifrifol ar fusnes.
- Bydd cynllunio ar gyfer parhad busnes yn cynnwys camau i glustnodi a lleihau'r risgiau, cyfyngu ar y canlyniadau os digwydd achos o dorri rheolau, a sicrhau bod gweithdrefnau hanfodol yn cael eu hadfer yn gyflym.
- Gweithio gyda'r Gwasanaethau TGCh i sefydlu parthau gwaith Parhad Busnes lle y bo'n ofynnol gan y gwasanaeth.
- Sicrhau bod gweithdrefnau wedi'u sefydlu i sicrhau bod y gwasanaethau yn parhau drwy gydol y cyfnod adfer.
- Yr holl faterion diogelwch gan gynnwys caniatadau mynediad a diogelwch gwybodaeth ar bapur.
- Sicrhau bod Perchnogion System yn cadw cofrestr o ddefnyddwyr y system fel bod mynediad i hawliau yn gallu cael ei reoli'n gywir.
- Sicrhau bod pob newid a wneir i'r system yn cael ei gofnodi'n ffurfiol drwy weithdrefn rheoli newidiadau a'u bod yn cael eu hadolygu i sicrhau nad ydynt yn peryglu diogelwch naill ai'r system neu'r amgylchedd gweithredu.

4.4 Mae'r Gwasanaethau TGCh yn gyfrifol am:

- Cadw rhestr o'r holl systemau gweinyddu craidd, strategaethau wrth gefn a swyddogion ar gyfer rhoi'r gweithdrefnau wrth gefn ar waith.
- Goruchwylio a chydlynu materion aml-lwyfan sy'n ymwneud â diogelwch cyfrifiadurol.
- Helpu perchnogion systemau, cyn dyfarnu contract i unrhyw gontractwr allanol, fod eu contract yn dibynnu ar gydymffurfio â'r holl fesurau diogelwch perthnasol.
- Sefydlu gweithdrefnau ar gyfer rheoli digwyddiadau lle tresmaswyd ar y system a bygythiadau maleisus ar feddalwedd.
- Sicrhau diogelwch yr holl gyfrifiaduron, gan gynnwys gweinyddion sy'n cefnogi system a'i data a dyfeisiau defnyddiwr.
- Datblygu a chynnal cynlluniau wrth gefn rhag argyfwng fydd yn cynnwys enwebu staff penodol i fod yn gyfrifol am weithredu'r camau wrth gefn ac adfer.
- Sicrhau bod staff y Gwasanaethau TGCh yn cael hyfforddiant priodol mewn ymwybyddiaeth diogelwch.
- Mewn cydweithrediad â rheolwyr llinell, sefydlu a chyfathrebu'r mesurau diogelwch sy'n ofynnol i ddiogelu eu rhaglenni. Mae'r cyfrifoldeb hwn yn cynnwys mesurau diogelwch ar gyfer caledwedd, meddalwedd, cyfathrebu a phersonél.
- Nodi'r gofynion diogelwch pan fo system sydd i'w gweithredu yn cael ei dylunio. Bydd rheolaethau diogelwch priodol, gan gynnwys llwybrau archwilio a phrosesu wrth gefn, yn cael eu dylunio'n rhan o raglenni. Efallai y bydd angen gwrthfesurau ychwanegol ar gyfer systemau sy'n prosesu data sensitif, gwerthfawr, neu gritigol, neu sy'n cael effaith arnynt.
- Gwerthuso cynnyrch diogelwch ac argymell atebion i broblemau diogelwch aml-lefel.
- Sicrhau bod strategaeth diogelwch seiber gadarn a thrylwyr ar waith
- Cadw cofnod o weithgarwch y rhwydwaith a chael mynediad i gofnodion i'w defnyddio wrth ymchwilio i achos o dorri rheolau neu ddigwyddiad diogelwch am gyfnod o 6 mis
- Bod yn ymwybodol o statws diogelwch cyfredol y prif systemau a'r problemau a allai godi. Bydd hyn yn cynnwys comisiynu profion diogelwch, profion ymdreiddiad ac archwiliadau diogelwch mewnol.
- Bod yn ymwybodol o ddatblygiadau technolegol newydd ac ymchwilio i werth y datblygiadau hynny.

4.5 Bydd y Swyddog Diogelwch Digidol:

Yn goruchwylio'r modd y caiff yr holl reolaethau diogelwch TG eu rhoi ar waith a'u monitro, a bydd hefyd yn cynghori ar ddatblygu strategaethau ar gyfer y dyfodol.

4.6 Adnoddau Dynol

Rhaid mynd i'r afael â diogelwch wrth recriwtio a dylid ei gynnwys mewn disgrifiadau swydd, contractau ac ar bob cwrs cynefino. Dylai disgrifiadau swydd ddiffinio'r cyfrifoldebau o ran diogelwch, fel y nodir ym Mholisi Diogelwch Gwybodaeth y Cyngor. Dylai hyn gynnwys unrhyw gyfrifoldebau cyffredinol am weithredu neu am gynnal Polisi Diogelwch Gwybodaeth y Cyngor, yn ogystal ag unrhyw gyfrifoldeb penodol am warchod systemau penodol neu am roi prosesau diogelwch ar waith.

5. Rheoli Mynediad

5.1 Adnabod a dilysu defnyddwyr

Rhaid i'r mynediad i asedau gwybodaeth fod yn gyfyngedig i ddefnyddwyr awdurdodedig, a rhaid eu diogelu trwy ddulliau rheoli priodol.

Bydd y rhain yn cynnwys y canlynol, heb fod yn gyfyngedig iddynt:

- Cyfyngiadau ffisegol i adeiladau'r Cyngor megis systemau mynediad trwy gerdyn adnabod
- Prosesau adnabod cadarn i gael mynediad i rwydwaith y Cyngor trwy ddilysu pwy yw'r defnyddiwr
- Gorfodi caniatâd mynediad i ddata electronig, gan weithredu yn ôl yr egwyddor y fraint leiaf

5.2 Mynediad i ddefnyddwyr

Rhaid i Berchnogion Asedau Gwybodaeth sicrhau bod mynediad i asedau gwybodaeth yn cael ei gyfyngu yn ôl swyddogaeth benodol y defnyddiwr Rhaid i fynediad fod yn seiliedig ar y breintiau lleiaf sydd eu hangen arnynt i wneud eu gwaith.

Rhaid i ddefnyddwyr gyrchu asedau gwybodaeth dim ond pan fydd angen iddynt wneud hynny er mwyn cyflawni eu swydd neu orchwyl penodol a neilltuir iddynt. Ystyrir bod mynediad bwriadol i asedau gwybodaeth y tu allan i'r sefyllfaoedd hyn yn anawdurdodedig a heb gydsyniad y Cyngor.

Mae mynediad anawdurdodedig i wybodaeth yn torri amodau'r polisi hwn a gall arwain at gymryd camau disgyblu.

Gall hyn hefyd fod yn gyfystyr â thorri'r Rheoliad Diogelu Data Cyffredinol a Deddf Camddefnyddio Cyfrifiaduron 1990, a gall fod yn fater digon difrifol i adrodd amdano wrth y Comisiynydd Gwybodaeth a gall arwain at erlyn y defnyddiwr dan sylw.

5.3 Rheoli cyfrineiriau

Rhaid i bob cyfrinair a ddefnyddir i gael mynediad i asedau gwybodaeth gael ei gadw'n gyfrinachol, a rhaid ei newid yn rheolaidd yn unol â'r arweiniad isod ynghylch cyfrineiriau:

http://intranet/our-people/it-support/manage-your-password/.

5.4 Terfynu mynediad, ei addasu neu ei ddiddymu

Rhaid i reolwyr llinell nodi unrhyw newidiadau i swyddogaeth unigolion sy'n effeithio ar eu hanghenion i gael mynediad i wybodaeth a rhaid rhoi gwybod i'r Gwasanaethau TGCh amdanynt yn syth.

Mae gan ddefnyddwyr hefyd gyfrifoldeb i roi gwybod i'r Gwasanaethau TGCh a'u rheolwr llinell am unrhyw wrthdaro buddiannau y maent yn ymwybodol ohono ac a allai godi, a fyddai'n effeithio ar rôl eu swydd a'u mynediad i wybodaeth.

Pan fydd staff yn gadael cyflogaeth y Cyngor, gan gynnwys lle caiff gweithwyr eu gwahardd, bydd y Tîm Adnoddau Dynol yn gwneud yn siŵr bod Gwasanaethau TGCh y Cyngor yn cael gwybod yn ddiymdroi i sicrhau bod y caniatâd mynediad yn cael ei derfynu.

Mae Rheolwyr Llinell yn gyfrifol am sicrhau y rhoddir gwybod i weinyddwyr systemau (e.e. *Ohms, CareFirst* ac ati) am yr angen i waredu cyfrifon lle mae mynediad wedi ei derfynu/atal dros dro.

5.5 Mynediad trydydd parti

Rhaid i bob mynediad gan drydydd parti (contractwyr, partneriaid busnes, ymgynghorwyr, gwerthwyr, cwsmeriaid) gael ei awdurdodi a'i fonitro'n briodol. Caniateir mynediad gan drydydd parti i asedau gwybodaeth fesul cyfnodau o 6 mis neu lai. Mewn achosion lle mae angen mynediad am gyfnodau hirach, rhaid i berchnogion y busnes nodi amserlenni mynediad a chyfiawnhad dros fynediad o'r fath.

5.6 Proseswyr Data

Dim ond ar ôl cael sicrwydd digonol y bydd gofynion y Rheoliad Diogelu Data Cyffredinol yn cael eu bodloni, ac y bydd hawliau'r rheiny sy'n destun y data yn cael eu gwarchod, y caiff unrhyw drydydd parti fynediad i ddata personol er mwyn ei brosesu ar ran y Cyngor. Rhaid i'r Proseswyr weithredu'n unig yn ôl cyfarwyddiadau cofnodedig y Cyngor, o dan gontract ysgrifenedig rhwymol (Cytundeb Prosesu Data). Rhaid i wasanaethau a ddarperir gan drydydd partïon gynnwys trefniadau diogelwch cytûn, diffiniadau o'r gwasanaeth a chytundebau cyflawni gwasanaeth.

5.7 Monitro systemau

Caiff mynediad i systemau hanfodol ei gofnodi, ynghyd â'r defnydd ohonynt, i ganfod unrhyw achosion o beidio â chydymffurfio â'r mesurau rheoli mynediad a nodir yn y polisi hwn, ac i gofnodi tystiolaeth mewn achosion o beidio â chydymffurfio/digwyddiadau'n ymwneud â diogelwch.

Rhaid adolygu'r cofnodion yn rheolaidd.

5.8 Archwiliadau

Bydd archwiliadau'n cael eu cynnal yn y Cyngor yn rheolaidd i ddilysu'r lefelau mynediad ac i sicrhau cydymffurfiaeth.

6. Diogelwch ffisegol ac amgylcheddol

6.1 Mannau diogel

Rhaid lleoli unrhyw gyfryngau, gan gynnwys offer TGCh, sydd â gwybodaeth sensitif (e.e. gwybodaeth bersonol) mewn mannau diogel. Rhaid bod diogelwch ffisegol rhag mynediad hab ganiatâd, difrod ac ymyrraeth (e.e. drysau wedi'u cloi). Caiff y rhain eu gosod mewn mannau diogel wedi'u gwarchod gan ffin ddiogelwch benodol gyda rheolaethau mynediad priodol a rhwystrau diogelwch (e.e. rhaniad ar gyfer desgiau/waliau, mynediad drwy gerdyn ac ati.).

6.2 Clirio sgrin a chlirio desg

Er mwyn sicrhau diogelwch gwybodaeth, rhaid clirio gwybodaeth sensitif o ddesgiau a swyddfeydd (er enghraifft, gwybodaeth bersonol). Hefyd, rhaid i sgriniau cyfrifiaduron personol fod yn glir o unrhyw wybodaeth pan na fydd rhywun wrth y ddesg neu yn y swyddfa. Dylai defnyddwyr sicrhau eu bod wedi allgofnodi o offer TG os byddant yn ei adael.

7. Rheolaethau Diogelwch Gweithredol

7.1 Gweithdrefnau gweithredu wedi'u dogfennu

Er mwyn sicrhau bod cyfleusterau prosesu gwybodaeth cywir a diogel ar waith, paratoir gweithdrefnau ar gyfer gweithgareddau system megis cychwyn a therfynu, gweithdrefnau wrth gefn, adfer a chynnal a chadw.

7.2 Rheoli Asedau Offer TGCh

Mae'r gwasanaethau TGCh yn cadw tystiolaeth ddogfennol o'r holl offer a meddalwedd cyfrifiadurol. Rhaid cadw'r cofnodion hyn er cywirdeb.

- Rhaid i bob eitem ar y rhestr ddangos pob ased TGCh yn glir drwy gyfrwng tag adnabod sy'n cynnwys ei rif ased unigryw
- Dim ond drwy'r Gwasanaethau TGCh y gellir prynu offer a meddalwedd TGCh
- Ni ddylid gosod unrhyw offer ar rwydwaith y Cyngor heb ganiatâd y Gwasanaethau TGCh ymlaen llaw
- Yn achos unrhyw offer a werthir, rhaid gwneud hynny drwy'r Gwasanaethau TGCh a'i gofnodi.

7.3 Rheoli Newid

Bydd y Gwasanaethau TGCh yn dilyn gweithdrefnau rheoli newid wedi'u dogfennu er mwyn galluogi adnabod a chofnodi newidiadau sylweddol. Rhaid i'r weithdrefn ystyried cynllunio a phrofi newidiadau, asesu effeithiau posibl, gweithdrefn gymeradwyo ffurfiol ar gyfer newidiadau arfaethedig, cyfathrebu manylion y newid i bartïon perthnasol a gweithdrefnau wrth gefn.

7.4 Gwahanu dyletswyddau

Lle bynnag y bo'n ymarferol a phosibl, dylid gwahanu dyletswyddau. Er enghraifft, dylai'r sawl sy'n gyfrifol am symbylu digwyddiadau fod yn wahanol i'r sawl sy'n gyfrifol am eu hawdurdodi.

7.5 Cynllunio Systemau a'u Derbyn

Er mwyn lleihau'r perygl y gallai systemau fethu, bydd dulliau rheoli yn cael eu rhoi ar waith i reoli'r capasiti ac i dderbyn systemau.

7.6 Gwarchod rhag codau maleisus a symudol

Er mwyn diogelu rhag difrod gan god maleisus a symudol fel firysau cyfrifiadurol, bydd yr awdurdod yn gweithredu systemau a rheolaethau i atal gweithredu cod diawdurdod ar systemau. Mae'r rheolaethau hyn yn cynnwys, ond heb eu cyfyngu i, gwaredu hawliau gweinyddol, gwrthfirws endpoint, hidlo e-bost a rhyngrwyd, a System Atal/Canfod Tresmasu ar ein porth i'r rhyngrwyd.

7.7 Copïau wrth gefn

Bydd copïau wrth gefn yn cael eu gwneud o ddata hollbwysig a bydd y system wrth gefn yn cael ei chofnodi a'i phrofi i sicrhau bod modd adfer yr holl wybodaeth a'r feddalwedd hanfodol ar ôl argyfwng neu os bydd y cyfryngau yn methu.

7.8 Rheoli diogelwch rhwydwaith

Bydd y Gwasanaethau TG yn rhoi dulliau rheoli ar waith i sicrhau diogelwch y wybodaeth mewn rhwydweithiau ac i ddiogelu gwasanaethau cysylltiedig rhag i rywun gael mynediad iddynt heb awdurdod.

Er mwyn sicrhau bod mynediad Wi-Fi yn cael ei osod, ei gynnal a'i gadw a'i ddefnyddio yn ddiogel, a lle bo angen busnes am hynny, bydd offer rhwydweithio di-wifr cymeradwy yn cael ei osod gan y Gwasanaethau TGCh neu drydydd partïon cymeradwy.

Bydd mynediad di-wifr i'r rhwydwaith corfforaethol yn cael ei gyfyngu i ddyfeisiau corfforaethol a bydd angen ei ddilysu.

Rhaid i offer rhwydweithio di-wifr a rhyngwynebau rheoli fod yn ddigon diogel i atal mynediad heb awdurdod.

Cynhelir archwiliadau rheolaidd o rwydweithiau di-wifr a bydd unrhyw bwyntiau mynediad anawdurdodedig yn cael eu dileu.

7.9 Caffael, datblygu a chynnal a chadw systemau gwybodaeth

Ni ddylid caffael Systemau Gwybodaeth heb gael caniatâd pendant gan y Gwasanaethau TGCh i sicrhau bod systemau yn ddiogel ac yn cyd-fynd â'n seilwaith TGCh. Mae hyn yn cynnwys systemau gweithredu, seilwaith, ceisiadau busnes, cynhyrchion oddi ar y silff, gwasanaethau a rhaglenni a ddatblygwyd gan y defnyddiwr sy'n cefnogi'r broses fusnes. Dylid clustnodi'r gofynion diogelwch a chytuno arnynt cyn datblygu a/neu weithredu systemau gwybodaeth.

8. Mesur Cydymffurfiaeth

Mae cydymffurfio â'r Polisi Diogelwch Gwybodaeth hwn yn orfodol.

9. Noddwr

Eiddo'r Grŵp Llywodraethu Gwybodaeth Corfforaethol yw'r polisi hwn.

10. Ceidwad

Cyfrifoldeb y Swyddog Diogelwch Digidol yw sicrhau bod y polisi yn cael ei adolygu a'i ddiweddaru'n rheolaidd.

11. Sicrhau triniaeth gyfartal

Bydd yn rhaid rhoi'r polisi hwn ar waith yn gyson heb ystyried hil, lliw, cenedl, tarddiad ethnig neu genedlaethol, iaith, anabledd, crefydd, oedran, rhyw, trosglwyddiad rhyw, tueddfryd rhywiol, statws priodasol na chyfrifoldebau magu plant.

Cymeradwywyd y Polisi gan y Bwrdd Gweithredol ar:	22 Hydref 2018
Adolygu'r Polisi:	1 Ebrill 2023
Ysgrifennwyd y polisi gan:	Richard R Williams a John M Williams (CISMP)