



National Cyber  
Security Centre  
a part of GCHQ



# Cyber Essentials: Gofynnion ar gyfer seilwaith TG f3.1

Ebrill 2023

© Hawlfraint y Goron 2023

## Cynnwys

Beth sy'n newydd yn y fersiwn hon .....	3
A. Cyflwyno'r rheolaethau technegol .....	3
B. Diffiniadau.....	3
C. Cwmpas.....	4
Trosolwg o'r cwmpas .....	4
Rheoli asedau a Cyber Essentials .....	4
(i) Dod â'ch dyfais eich hun (BYOD) .....	5
(ii) Gweithio gartref.....	6
(iii) Dyfeisiau di-wifr .....	6
(iv) Gwasanaethau cwmwl .....	6
(v) Cyfrifon a ddefnyddir gan drydydd partïon a seilwaith a reolir.....	7
(vi) Dyfeisiau a ddefnyddir gan drydydd partïon .....	7
(vii) Cymwysiadau ar y we.....	8
D. Gofynion yn ôl thema rheolaeth dechnegol.....	8
1. Waliau Tân .....	8
Nod.....	8
Cyflwyniad.....	8
Gofynion.....	9
2. Ffurfweddiad diogel .....	9
Nod.....	9
Cyflwyniad.....	9
Gofynion.....	10
3. Rheoli diweddariadau diogelwch.....	10
Nod.....	10
Cyflwyniad.....	11
Gofynion.....	11
4. Rheoli mynediad defnyddwyr .....	11
Nod.....	11
Cyflwyniad.....	12
Gofynion.....	12
Dilysu drwy gyfrinair .....	13
Dull dilysu aml-ffactor.....	13
5. Amddiffyn rhag maleiswedd .....	14

Nod.....	14
Cyflwyniad.....	14
Gofynion.....	14
D. Canllawiau pellach.....	15
Creu copi wrth gefn o'ch data.....	15
Dim Ymddiriedaeth a Cyber Essentials .....	15

## Beth sy'n newydd yn y fersiwn hon

- Mae'r diffiniad o 'feddalwedd' wedi'i ddiweddu er mwyn egluro ble mae cadarnwedd yn y cwmpas
- Datganiad yn esbonio pam mae rheoli asedau yn bwysig ym maes Cyber Essentials
- Mae dolen i ganllawiau'r Ganolfan Seiberddiogelwch Genedlaethol ar ddod â'ch dyfais eich hun wedi'i hychwanegu er gwybodaeth
- Eglurhad ar gynnwys dyfeisiau trydydd parti
- Mae'r adran ar ddatgloi dyfeisiau wedi'i diweddu er mwyn adlewyrchu'r ffaith na ellir addasu rhai ffurfwediadau oherwydd cyfyngiadau gwerthwyr
- Mae'r adran ar amddiffyn rhag maleiswedd wedi'i diweddu
- Gwybodaeth newydd am sut mae defnyddio saerniâeth dim ymddiriedaeth yn effeithio ar Cyber Essentials

## A. Cyflwyno'r rheolaethau technegol

Rydym wedi trefnu'r gofynion o dan bum rheolaeth dechnegol:

1. Waliau Tân
2. Ffurfwediad diogel
3. Rheoli diweddariadau diogelwch
4. Rheoli mynediad defnyddwyr
5. Amddiffyn rhag maleiswedd

Fel sefydliad sy'n gwneud cais am ardystiad o dan gynllun Cyber Essentials, eich cyfrifoldeb chi yw sicrhau bod eich sefydliad yn bodloni'r holl ofynion. Mae'n bosibl hefyd y bydd angen i chi ddarparu tystiolaeth cyn y gall eich corff ardystio roi tystysgrif i chi ar y lefel rydych yn gwneud cais amdani.

Beth y dylech ei wneud gyntaf:

- Pennu **ffin y cwmpas** ar gyfer eich sefydliad, ac yna **bennu beth yw'r cwmpas o fewn y ffin hon**.
- Adolygu pob un o'r **pum thema rheolaeth dechnegol a'r rheolaethau y maent yn eu corffor fel gofynion**.
- Cymryd y camau angenrheidiol i **sicrhau bod eich sefydliad yn bodloni pob gofyniad** sydd ei angen arno ar gyfer y cwmpas a benwyd gennych.

## B. Diffiniadau

- Mae **meddalwedd** yn cynnwys systemau gweithredu, cymwysiadau masnachol parod, ategion, dehonglwyr, sgriftiau, llyfrgelloedd, meddalwedd rhwydwaith a wal dân a chadarnwedd llwybrydd.
- Mae **dyfeisiau** yn cynnwys pob math o westeiwyr, cyfarpar rhwydweithio, gweinyddion, rhwydweithiau, a dyfeisiau defnyddiwr terfynol, megis cyfrifiaduron bwrdd gwaith, gliniaduron, cleientiaid tenau, llechi a ffonau clyfar — boed yn ffisegol neu'n rhithwir.
- Mae **ymgeisydd** yn cyfeirio at eich sefydliad sy'n ceisio ardystiad, neu weithiau'r unigolyn sy'n gweithredu fel y prif bwynt cyswllt, yn dibynnu ar y cyd-destun.
- Rhwydwaith preifat rhithwir yw **VPN corforaethol** sy'n cysylltu yn ôl i leoliad eich swyddfa, neu i wal dân rithwir neu ar y cwmwl. Mae'n rhaid i chi weinyddu'r VPN fel y gallwch gymhwysu rheolaethau'r wal dân.

- Mae **data sefydliadol** yn cynnwys unrhyw ddata electronig sy'n perthyn i'ch sefydliad, er enghraifft, negeseuon e-bost, dogfennau, data cronfa ddata, data ariannol.
- Mae **gwasanaeth sefydliadol** yn cynnwys unrhyw gymwysiadau meddalwedd, cymwysiadau cwmwl, gwasanaethau cwmwl, byrddau gwaith rhngweithiol defnyddwyr a datrysiau rheoli dyfeisiau symudol y mae eich sefydliad yn berchen arnynt neu'n tansysgrifio iddynt. Er enghraifft: cymwysiadau ar y we, Microsoft 365, Google Workspace, cynwsysydion rheoli dyfeisiau symudol, Citrix Desktop, datrysiau Virtual Desktop neu deleffoni IP.
- Mae **is-set** yn rhan o'r sefydliad y mae ei rwydwaith wedi'i wahanu oddi wrth weddill y sefydliad gan wal dân neu rwydwaith ardal leol rithwir (VLAN).
- Dyfeisiau yw **gweinyddion** sy'n darparu data sefydliadol neu wasanaethau i ddyfeisiau eraill fel rhan o fusnes eich sefydliad.
- Meddalwedd y mae gennych hawl gyfreithiol i'w defnyddio yw **meddalwedd drwyddedig a gefnogir** ac y mae gwerthwr wedi ymrwymo i'w chefnogi drwy ddarparu diweddarriadau neu batsys rheolaidd. Mae'n rhaid i'r gwerthwr ddarparu dyddiad yn y dyfodol pan na fydd yn darparu diweddarriadau mwyach. (Noder nad oes rhaid i'r gwerthwr fod wedi creu'r feddalwedd yn y lle cyntaf, ond rhaid iddo allu addasu'r feddalwedd wreiddiol er mwyn creu diweddarriadau).

## C. Cwmpas

### Trosolwg o'r cwmpas

Dylai eich asesiad a'ch ardystiad gwmpasu'r seilwaith TG cyfan a ddefnyddir i gyflawni busnes eich sefydliad neu, os oes angen, is-set a reolir ar wahân ac wedi'i diffinio'n dda. Y naill ffordd neu'r llall, mae'n rhaid i chi ddiffinio ffin y cwmpas yn glir, sef: yr uned fusnes sy'n ei reoli, ffin y rhwydwaith a'r lleoliad ffisegol. Rhaid i chi gytuno ar y cwmpas â'r corff ardystio cyn dechrau'r asesiad.

Gellir defnyddio is-set i ddiffinio beth sydd **yn y cwmpas a'r tu allan i'r cwmpas** ar gyfer eich ardystiad Cyber Essentials.

**Noder:** *Sefydladau sy'n dewis cwmpas sy'n cynnwys eu seilwaith TG cyfan sy'n cyflawni'r amddiffyniad gorau ac yn sicrhau hyder eu cwsmeriaid.*

Mae'r gofynion yn berthnasol i bob dyfais a meddalwedd yn y cwmpas ac sy'n bodloni unrhyw un o'r amodau hyn:

- gallu derbyn cysylltiadau â'r rhwydwaith sy'n dod i mewn gan westeiwyr annibynadwy sydd wedi cysylltu â'r rhyngrwyd
- gallu sefydlu cysylltiadau allan a ysgogir gan y defnyddiwr â dyfeisiau drwy'r rhyngrwyd
- rheoli llif data rhwng unrhyw un o'r dyfeisiau uchod a'r rhyngrwyd.

Nid yw cwmpas nad yw'n cynnwys dyfeisiau defnyddwyr terfynol yn dderbyniol.

### Rheoli asedau a Cyber Essentials

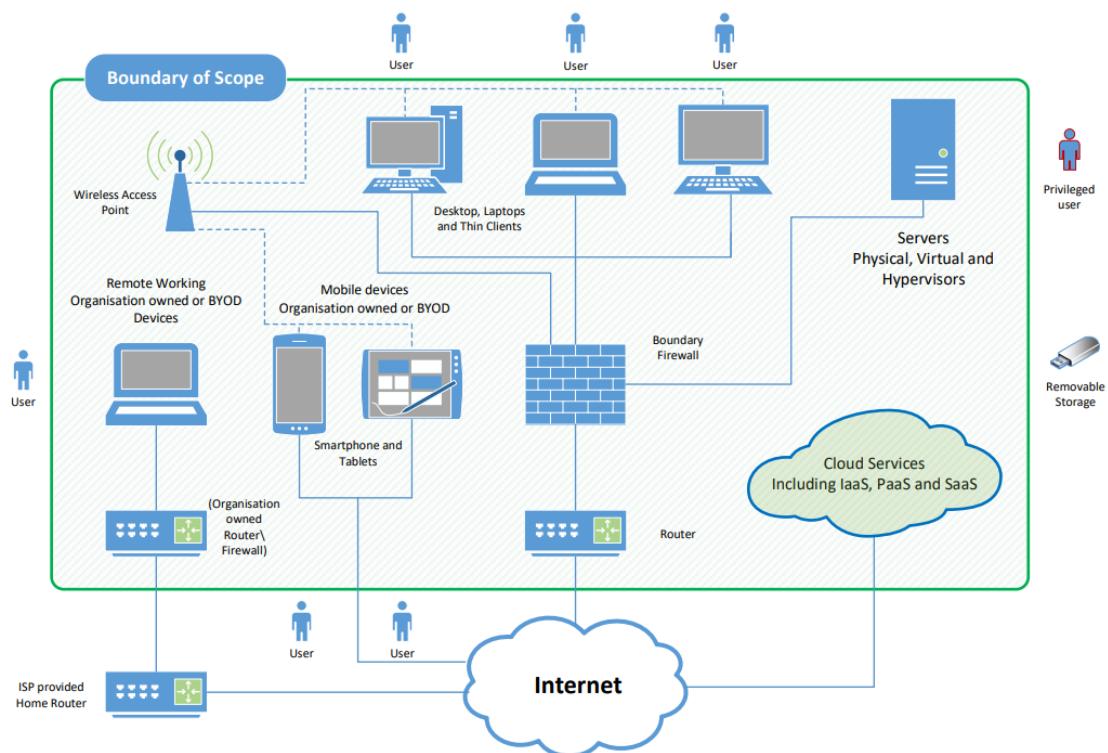
Nid yw rheoli asedau yn un o reolaethau penodol Cyber Essentials, ond gall rheoli asedau yn effeithiol helpu i fodloni'r pum rheolaeth, felly dylid ei ystyried fel swyddogaeth diogelwch craidd.

Mae'r rhan fwyaf o weithrediadau busnes yn dibynnu ar ryw agwedd ar reoli asedau, ac ni ddylid ystyried seiberddiogelwch ar ei ben ei hun, neu fel prif ddefnyddiwr gwybodaeth asedau. Mae'r swyddogaethau hyn yn cynnwys gweithrediadau TG, cyfrifyddu ariannol, trwyddedau rheoli meddalwedd, caffaol a logisteg. Mae'n bosibl na fydd angen yr un wybodaeth ar bob un, ond bydd y gofynion perthnasol yn gorgyffwrdd ac yn rhannu dibyniaethau. Bydd integreiddio a chydgylltu

prosesau rheoli asedau ar draws eich sefydliad yn helpu i leihau neu reoli unrhyw achosion o wrthdaro rhwng y swyddogaethau hyn.

Nid yw rheoli asedau yn effeithiol yn golygu creu rhestrau neu gronfeydd data na chânt eu defnyddio fyfth. Mae'n golygu creu, sefydlu a chynnal gwybodaeth awdurdodol a chywir am eich asedau sy'n galluogi gweithrediadau o ddydd i ddydd a phrosesau gwneud penderfynu effeithlon pan fydd eu hangen arnoch. Yn benodol, bydd yn eich helpu i olrhain a rheoli dyfeisiau wrth iddynt gael eu cyflwyno i'ch busnes.

Mae gan y Ganolfan Seiberddiogelwch Genedlaethol [ganllawiau cynhwysfawr i sefydliadau ar reoli asedau](#).



Ffigur 1: Cwmpas y gofynion ar gyfer seilwaith TG

### (i) Dod â'ch dyfais eich hun (BYOD)

Yn ogystal â dyfeisiau symudol neu ddyfeisiau o bell y mae'r sefydliad yn berchen arnynt, mae dyfeisiau y mae defnyddwyr yn berchen arnynt sy'n cael mynediad at ddata neu wasanaethau'r sefydliad (fel y'u diffinnir uchod) hefyd **yn rhan o'r cwmpas**. Fodd bynnag, mae'r holl ddyfeisiau symudol neu ddyfeisiau o bell a ddefnyddir at y dibenion canlynol **yn unig**:

- cymwysiadau llais brodorol
- cymwysiadau testun brodorol
- cymwysiadau diliysu aml-ffactor

### y tu allan i'r cwmpas.

Yn draddodiadol, roedd dyfeisiau defnyddwyr yn cael eu rheoli'n fewnol, a oedd yn sicrhau cysondeb ym mhob rhan o'r sefydliad. Mae ardystio rheolaethau diogelwch yn y ffordd hon yn symlach gan fod gwneuthuriad safonol y gellir cyfeirio ato.

Mae BYOD yn cymhlethu pethau, gan fod defnyddwyr yn cael mwy o ryddid i 'addasu' eu profiad sy'n golygu bod rhoi'r rheolaethau ar waith mewn ffordd gyson yn fwy heriol. Dylai defnyddio'r diffiniadau o ran data a gwasanaethau sefydliadol i orfodi polisiau mynediad cryf ddileu rhywfaint o'r amwysedd hwn.

I gael rhagor o [wybodaeth a chyngor ar ddefnyddio BYOD](#), gweler canllawiau'r Ganolfan Seiberddiogelwch Genedlaethol.

#### (ii) Gweithio gartref

Ein dull gweithredu diofyn yw bod pob dyfais gweithio gartref gorfforaethol neu BYOD a ddefnyddir ar gyfer busnes eich sefydliad o fewn cwmpas Cyber Essentials.

Os bydd eich sefydliad yn rhoi llwybrydd i'r sawl sy'n gweithio gartref, bydd y llwybrydd hwnnw'n rhan o'r cwmpas hefyd.

Bydd pob llwybrydd arall **y tu allan i'r cwmpas** sy'n golygu y bydd angen i chi roi rheolaethau wal dŵn Cyber Essentials (megis wal dŵn meddalwedd) ar ddyfeisiau defnyddwyr.

Os bydd y sawl sy'n gweithio gartref yn defnyddio VPN corfforaethol, bydd ei ffin rhyngrwyd ar wal dŵn y cwmni neu wal dŵn rithwir/ar y cwmwl.

#### (iii) Dyfeisiau di-wifr

Mae dyfeisiau di-wifr (gan gynnwys pwyntiau mynediad di-wifr):

- **o fewn y cwmpas** os gallant gyfathrebu â dyfeisiau eraill drwy'r rhyngrwyd
- **y tu allan i'r cwmpas** os nad yw'n bosibl i ymosodwr ymosod yn uniongyrchol drwy'r rhyngrwyd (nid yw cynllun Cyber Essentials yn ymwneud ag ymosodiadau y gellir ond eu lansio o fewn ystod signal y ddyfais ddi-wifr)
- **y tu allan i'r cwmpas** os ydynt yn rhan o lwybrydd ISP yn y cartref

#### (iv) Gwasanaethau cwmwl

Os caiff data neu wasanaethau eich sefydliad eu lletya ar wasanaethau cwmwl, rhaid i'r gwasanaethau hyn fod **o fewn y cwmpas**.

Ar gyfer gwasanaethau cwmwl, **y sefydliad sy'n gwneud cais sydd bob amser yn gyfrifol** am sicrhau y caiff pob rheolaeth ei rhoi ar waith, ond gall rhai o'r rheolaethau gael eu rhoi ar waith gan ddarparwr y gwasanaeth cwmwl. Mae pwys yn rhoi pa reolaeth ar waith yn dibynnu ar y math o wasanaeth cwmwl. Rydym yn ystyried tri math gwahanol o wasanaeth cwmwl:

- **Seilwaith fel Gwasanaeth (IaaS)** – bydd darparwr y cwmwl yn darparu gweinyddion rhithwir a chyfarpar rhwydwaith a gaiff eu ffurfweddu a'u rheoli gan eich sefydliad, yn debyg i gyfarpar ffisegol. Mae enghreifftiau o IaaS yn cynnwys Rackspace, Google Compute Engine, neu Amazon EC2.
- **Llwyfan fel Gwasanaeth (PaaS)** – bydd darparwr y cwmwl yn darparu ac yn rheoli'r seilwaith sylfaenol, a bydd eich sefydliad yn darparu ac yn rheoli'r cymwysiadau. Mae enghreifftiau o PaaS yn cynnwys Azure Web Apps ac Amazon Web Services Lambda.
- **Meddalwedd fel Gwasanaeth (SaaS)** – bydd darparwr y cwmwl yn darparu cymwysiadau, a bydd eich sefydliad yn ffurfweddu'r gwasanaethau wedyn. Mae'n rhaid i chi sicrhau bod y gwasanaeth yn cael ei ffurfweddu yn ddiogel. Mae enghreifftiau o SaaS yn cynnwys Microsoft 365, Dropbox a Gmail.

Bydd pwysy'n rhoi'r rheolaethau ar waith yn amrywio, yn dibynnu ar sut y mae'r gwasanaeth cwmwl wedi'i ddylunio. Mae'r tabl isod yn esbonio pwys y gellid disgwyl iddo roi pob rheolaeth ar waith fel arfer:

Gofyniad	IaaS	PaaS	SaaS
<b>Waliau Tân</b>	Eich sefydliad a darparwr y cwmwl	Darparwr y cwmwl a'ch sefydliad hefyd weithiau	Darparwr y cwmwl
<b>Ffurfweddiad diogel</b>	Eich sefydliad a darparwr y cwmwl	Eich sefydliad a darparwr y cwmwl	Eich sefydliad a darparwr y cwmwl
<b>Rheoli diweddfhariadau diogelwch</b>	Eich sefydliad a darparwr y cwmwl	Eich sefydliad a darparwr y cwmwl	Darparwr y cwmwl
<b>Rheoli mynediad defnyddwyr</b>	Eich sefydliad	Eich sefydliad	Eich sefydliad
<b>Amddiffyn rhag maleiswedd</b>	Eich sefydliad a darparwr y cwmwl	Darparwr y cwmwl a'ch sefydliad hefyd weithiau	Darparwr y cwmwl

Mewn achosion pan fydd darparwr y cwmwl yn rhoi un o'r rheolaethau ar waith ar eich rhan, mae'n rhaid i chi sicrhau bod darparwr y cwmwl wedi ymrwymo i roi hyn ar waith drwy gymalau contractiol neu ddogfennau y cyfeirir atynt yn y contract, megis datganiadau diogelwch neu ddatganiadau preifatrwydd. Bydd darparwyr cwmwl yn aml yn esbonio sut maent yn rhoi mesurau diogelwch ar waith mewn dogfennau a gyhoeddir yn eu canolfannau ymddiriedaeth, gan gyfeirio at 'fodel cyfrifoldeb a rennir'.

(v) Cyfrifon a ddefnyddir gan drydydd partiōn a seilwaith a reolir

Mae pob cyfrif y mae eich sefydliad yn berchen arno o fewn y cwmpas, hyd yn oed pan gaiff y cyfrifon hynny eu defnyddio gan drydydd parti, megis cyflenwr, contractwr neu Ddarparwr Gwasanaeth a Reolir (MSP) er mwyn rheoli neu gefnogi eich seilwaith.

Os ydych yn defnyddio gwasanaethau a reolir yn allanol (megis gwasanaeth gweinyddu o bell), rhaid i chi allu cadarnhau bod rheolaethau technegol Cyber Essentials yn cael eu bodloni, a dylech allu dangos hyn yn eich atebion i'r asesiad.

(vi) Dyfeisiau a ddefnyddir gan drydydd partiōn

Rhaid i bob dyfais defnyddiwr terfynol y mae eich sefydliad yn berchen arni sy'n cael ei rhoi ar fenthys i drydydd parti gael ei chynnwys yng nghwmpas yr asesiad.

Ar gyfer dyfeisiau nad yw eich sefydliad yn berchen arnynt, mae'r tabl isod yn esbonio beth sy'n rhan o'r cwmpas a beth sydd y tu allan iddo:

	Dyfeisiau y mae eich sefydliad yn berchen arnynt	Dyfeisiau y mae trydydd parti yn berchen arnynt	BYOD
<b>Gweithiwr</b>	<input checked="" type="checkbox"/>	Dd/G	<input checked="" type="checkbox"/>
<b>Gwirfoddolwr</b>	<input checked="" type="checkbox"/>	Dd/G	<input checked="" type="checkbox"/>
<b>Ymddiriedolwr</b>	<input checked="" type="checkbox"/>	Dd/G	<input checked="" type="checkbox"/>

<b>Cynorthwydd ymchwil mewn prifysgol</b>	<input checked="" type="checkbox"/>	Dd/G	<input checked="" type="checkbox"/>
<b>Myfyriwr</b>	<input checked="" type="checkbox"/>	Dd/G	<input checked="" type="checkbox"/>
<b>Gweinyddwr MSP</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Contractwr trydydd parti</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Cwsmer</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

O fewn y cwmpas

Y tu allan i'r cwmpas

Ar gyfer dyfeisiau y tu allan i gwmpas yr asesiad, bydd eich sefydliad yn gyfrifol o hyd am gadarnhau bod dyfeisiau sy'n rhwngweithio â gwasanaethau a data sefydliadol wedi'u ffurfweddu'n gywir. Mater i chi yw penderfynu sut i gyflawni hyn, gan ei fod y tu allan i gwmpas yr asesiad.

#### (vii) Cymwysiadau ar y we

Mae cymwysiadau masnachol ar y we sydd ar gael i'r cyhoedd (yn hytrach nag apiau a ddatblygir yn fewnol) yn rhan o'r cwmpas yn ddiofyn. Mae elfennau pwrrpasol ac wedi'u haddasu o gymwysiadau ar y we y tu allan i'r cwmpas. Y ffordd orau o liniaru gwendidau mewn cymwysiadau yw prosesau datblygu a phrofi cadarn yn unol ag arferion gorau masnachol, megis [Safon Dilysu Diogelwch Cymwysiadau OWASP | Sefydliad OWASP](#).

## D. Gofynion yn ôl thema rheolaeth dechnegol

### 1. Waliau Tân

**Yn gymwys i:** waliau Tân ffiniol, cyfrifiaduron bwrdd gwaith, gliniaduron, llwybryddion, gweinyddion, IaaS, PaaS, SaaS

Nod

Gwneud yn siŵr mai dim ond gwasanaethau rhwydwaith diogel ac angenrheidiol y gellir cael gafael arnynt drwy'r rhyngrwyd.

#### Cyflwyniad

Mae pob dyfais yn rhedeg gwasanaethau rhwydwaith i'w galluogi i gyfathrebu â dyfeisiau a gwasanaethau eraill. Drwy gyfyngu ar fynediad at y gwasanaethau hyn, byddwch yn llai agored i ymosodiadau. Gallwch wneud hyn drwy ddefnyddio waliau Tân neu ddyfeisiau rhwydwaith sydd â swyddogaeth wal dŵr. Ar gyfer gwasanaethau cwmwl, gallwch gyflawni hyn drwy ddefnyddio polisiau llif data.

Dyfais rhwydwaith yw wal dŵr ffiniol a all gyfyngu ar draffig rhwydwaith sy'n dod i mewn ac yn mynd allan o wasanaethau ar ei rwydwaith o gyfrifiaduron a dyfeisiau symudol. Gall helpu i amddiffyn rhag ymosodiadau seiber drwy roi cyfngiadau ar waith, a elwir yn 'rheolau wal dŵr', a all ganiatáu neu rwystro traffig yn dibynnu ar ei ffynhonnell, ei gyrchfan a'r math o brotocol cyfathrebu.

Fel arall, os nad yw eich sefydliad yn rheoli'r rhwydwaith y mae dyfais yn cysylltu ag ef, rhaid i chi ffurfweddu wal dŵr meddalwedd ar y ddyfais. Mae hon yn gweithio yn yr un ffordd â wal dŵr ffiniol ond bydd ond yn amddiffyn yr un ddyfais y mae wedi'i ffurfweddu arni. Mae'r dull gweithredu hwn yn caniatáu rheolau mwy penodol ac yn golygu bod y rheolau yn berthnasol i'r ddyfais lle bynnag y

caiff ei defnyddio. Ond dylech nodi bod hyn yn creu gorbenion gweinyddol mwy wrth reoli rheolau wal dân.

### Gofynion

Mae'n rhaid i chi amddiffyn pob dyfais o fewn y cwmpas gyda wal dân wedi'i ffurfweddu'n gywir (neu swyddogaeth wal dân ar gyfer dyfais rhwydwaith).

**Gwybodaeth:** Mae wal dân meddalwedd wedi'i rhagosod ar systemau gweithredu'r rhan fwyaf o gyfrifiaduron a gliniaduron bellach. Cynghorwn fod hon yn cael ei throi ymlaen i'r dewis cymhwysiad wal dân trydydd parti.

Ar gyfer pob wal dân (neu ddyfeisiau rhwydwaith â swyddogaeth wal dân), rhaid i'ch sefydliad wneud y canlynol:

- newid cyfrineiriau gweinyddol diofyn i gyfrinair cryf ac unigryw (gweler diliysu drwy gyfrinair)
  - neu analluogi mynediad gweinyddol o bell yn llwyr
- atal mynediad at y rhngwyneb gweinyddol (a ddefnyddir i reoli ffurfweddiad y wal dân) o'r rhngwyd, oni bai fod angen busnes clir ac wedi'i ddogfennu, a bod y rhngwyneb wedi'i amddiffyn gan un o'r rheolaethau canlynol:
  - dull diliysu aml-ffactor (gweler y manylion isod)
  - rhestr caniatáu IP sy'n cyfyngu mynediad i ystod fach o gyfeiriadau dibynadwy ynghyd â dull diliysu drwy gyfrinair a reolir yn briodol
- rhwystro cysylltiadau heb eu diliysu sy'n dod i mewn yn ddiofyn
- sicrhau bod rheolau wal dân sy'n dod i mewn yn cael eu cymeradwyo a'u dogfennu gan berson awdurdodedig, a chynnwys yr angen busnes yn y ddogfennaeth
- dileu neu analluogi rheolau wal dân diangen yn gyflym, pan na fydd eu hangen mwyach

Gwneud yn siŵr eich bod yn defnyddio wal dân meddalwedd ar ddyfeisiau a ddefnyddir ar rwydweithiau annibynadwy, megis llecynnau Wi-Fi cyhoeddus.

## 2. Ffurfweddiad diogel

**Yn gymwys i:** gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, cleientiaid tenau, IaaS, PaaS, SaaS

### Nod

Sicrhau bod cyfrifiaduron a dyfeisiau rhwydwaith wedi'u ffurfweddu'n briodol er mwyn:

- lleihau gwendidau
- darparu'r gwasanaethau sy'n ofynnol i gyflawni eu rôl yn unig

### Cyflwyniad

Nid yw ffurfweddiadau diofyn cyfrifiaduron a dyfeisiau rhwydwaith yn ddiogel bob amser. Bydd ffurfweddiadau safonol 'yn syth allan o'r bocs' yn aml yn cynnwys un man gwan neu fwy, megis:

- cyfrif gweinyddol sydd â chyfrinair diofyn wedi'i ragosod ac sy'n hysbys yn gyhoeddus, neu nad oes dull diliysu aml-ffactor wedi'i alluogi ar ei gyfer
- cyfrifon defnyddwyr sydd wedi'u rhag-alluogi ond sy'n ddiangen (weithiau gyda breintiau mynediad arbennig)
- cymwysiadau neu wasanaethau sydd wedi'u rhagosod ond sy'n ddiangen

Gall y gosodiadau diofyn hyn ganiatáu ymosodwyr i gael mynediad at wybodaeth sensitif eich sefydliad heb awdurdod.

Ond drwy ddefnyddio rhai rheolaethau technegol syml wrth osod cyfrifiaduron a dyfeisiau rhwydwaith, gallwch leihau gwendidau ac amddiffyn yn erbyn mathau cyffredin o ymosodiadau.

## Gofynion

### *Cyfrifiaduron a dyfeisiau rhwydwaith*

Mae'n rhaid i'ch sefydliad reoli eich cyfrifiaduron a'ch dyfeisiau rhwydwaith yn rhagweithiol. Mae'n rhaid i chi wneud y canlynol yn rheolaidd:

- dileu ac analluogi cyfrifon defnyddwyr diangen (megis cyfrifon gwesteion a chyfrifon gweinyddol na chânt eu defnyddio)
- newid unrhyw gyfrineiriau diofyn neu gyfrineiriau y gellir eu dyfalu ar gyfrifon (gweler diliysu drwy gyfrinair)
- dileu neu analluogi meddalwedd ddiangen (gan gynnwys cymwysiadau, cyfleustodau system a gwasanaethau rhwydwaith)
- analluogi unrhyw nodwedd sy'n rhedeg yn awtomatig sy'n caniatáu gweithredu ffeil heb awdurdodiad gan y defnyddiwr (er enghraifft, pan gaiff ei lawrlwytho)
- sicrhau bod defnyddwyr wedi'u diliysu cyn caniatáu iddynt gael mynediad at ddata neu wasanaethau sefydliadol
- sicrhau bod rheolaethau priodol ar gyfer cloi'r ddyfais (gweler 'datgloi dyfeisiau' isod) ar gyfer defnyddwyr sy'n bresennol yn gorfforol

### *Manylion ar gyfer datgloi dyfeisiau*

Os bydd angen presenoldeb corfforol defnyddiwr er mwyn cael mynediad at wasanaethau dyfais (megis mewngofnodi i liniadur neu ddatgloi ffôn symudol), rhaid i fanylion megis cyfrinair, PIN neu system fiometrig fod ar waith cyn y gall defnyddiwr gael mynediad at y gwasanaethau

Rhaid i chi ddiogelu eich dewis ddull diliysu (a all fod yn ddilysiad biometrig, drwy gyfrinair neu gyda PIN) rhag ymosodiadau grymus. Os bydd modd ffurfweddu, dylech ddefnyddio un o'r dulliau canlynol:

- cyfyngu ar nifer yr ymgeisiau, fel bod yr amser y mae'n rhaid i'r defnyddiwr aros rhwng ymgeisiau yn cynyddu gyda phob ymgais aflwyddiannus. Ni ddylech ganiatáu mwy na 10 cynnig mewn 5 munud
- cloi dyfeisiau ar ôl mwy na 10 ymgais aflwyddiannus.

Os na fydd y gwerthwr yn caniatáu i chi ffurfweddu'r uchod, defnyddiwr osodiad diofyn y gwerthwr.

Rhaid defnyddio rheolaethau technolegol i reoli ansawdd manylion. Os mai dim ond i ddatgloi dyfais mae manylion, defnyddiwr gyfrinair neu PIN sydd o leiaf 6 nod o hyd. Pan gaiff y manylion i ddatgloi'r ddyfais eu defnyddio ar gyfer diliysu hefyd, rhaid i chi ddefnyddio'r gofynion cyfrinair llawn a ddisgrifir yn 'rheolaethau mynediad defnyddwyr'.

## 3. Rheoli diweddariadau diogelwch

**Yn gymwys i:** weinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, waliau Tân, llwybryddion, IaaS, PaaS, SaaS

Nod

Sicrhau nad yw dyfeisiau a meddalwedd yn agored i broblemau diogelwch hysbys pan fo ffyrdd o'u hunioni ar gael.

## Cyflwyniad

Gall unrhyw ddyfais sy'n rhedeg meddalwedd gynnwys diffygion diogelwch, a elwir yn wendidau.

Deuir o hyd i wendidau mewn pob math o feddalwedd yn rheolaidd. Unwaith y deuir o hyd iddynt, bydd unigolion neu grwpiau maleisus yn symud yn gyflym i gamddefnyddio (neu 'gamfanteisio ar') wendidau er mwyn ymosod ar gyfrifiaduron a rhwydweithiau.

**Rhybudd:** *Bydd gwerthwyr cynhyrchion yn darparu ffyrdd o unioni gwendidau a nodir mewn cynhyrchion y maent yn dal i'w cefnogi ar ffurf diweddaradau meddalwedd a elwir yn 'batsys' neu'n ddiweddaradau diogelwch. Mae'n bosibl y darperir y rhain i gwsmeriaid yn syth neu'n unol ag amserlen ryddhau reolaidd (bob mis efallai).*

## Gofynion

Mae'n rhaid i chi sicrhau bod yr holl feddalwedd o fewn y cwmpas yn gyfredol. Mae'n rhaid i bob meddalwedd ar ddyfeisiau sydd o fewn y cwmpas:

- fod wedi'i thrwyddedu a'i chefnogi
- cael ei dileu oddi ar ddyfeisiau pan na fydd yn cael ei chefnogi mwyach neu pan gaiff ei dileu o'r cwmpas gan ddefnyddio is-set ddiffiniedig sy'n atal yr holl draffig i / o'r rhyngrywd
- bod â diweddaradau wedi'u galluogi lle bo'n bosibl
- cael ei diweddar, gan gynnwys gwneud unrhyw newidiadau ffurfweddu â llaw sy'n ofynnol er mwyn sicrhau bod y diweddarriad mewn grym, o fewn 14 diwrnod\* o ddiweddarriad yn cael ei ryddhau:
  - pan fo'r diweddarriad yn atgyweirio gwendidau a ddisgrifir gan y gwerthwr fel 'critigol' neu 'risg uchel'
  - pan fo'r diweddarriad yn ymdrin â gwendidau â sgôr sylfaen CVSS v3 o 7 neu fwy
  - nid oes unrhyw fanylion am lefel y gwendidau y mae'r diweddarriad a ddarperir gan y gwerthwr yn eu hatgyweirio

**Noder:** *Er mwyn bod mor ddiogel â phosibl, argymhellwn yn gryf (ond nid yw'n orfodol) fod yr holl ddiweddaradau a ryddhawyd yn cael eu rhoi ar waith o fewn 14 diwrnod i'w rhyddhau.*

\*Mae'n bwysig bod diweddaradau yn cael eu rhoi ar waith cyn gynted â phosibl. Ystyrrir bod 14 diwrnod yn gyfnod rhesymol i allu cyflawni'r gofyniad hwn. Byddai cyfnod hwy yn gyfystyr â risg ddiogelwch ddifrifol ac mae'n bosibl na fyddai cyfnod byrrach yn ymarferol.

**Gwybodaeth:** *Os bydd y gwerthwr yn defnyddio termau gwahanol i ddisgrifio difrifoldeb gwendidau, gweler y diffiniad manwl gywir yn y System Sgorio Gwendidau Cyffredin (CVSS). At ddiben y cynllun Cyber Essentials, gwendidau 'critigol' neu 'risg uchel' yw'r rheini sydd â sgôr CVSS3 o 7 neu uwch neu rai a nodir gan y gwerthwr fel 'critigol' neu 'risg uchel'.*

**Rhybudd:** *Bydd rhai gwerthwyr yn rhyddhau diweddaradau diogelwch ar gyfer sawl mater sy'n amrywio o ran difrifoldeb fel un diweddarriad. Os bydd unrhyw ddiweddarriad o'r fath yn cwmpasu materion 'critigol' neu 'risg uchel' yna rhaid ei osod o fewn 14 diwrnod.*

## 4. Rheoli mynediad defnyddwyr

**Yn gymwys i:** weinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, IaaS, PaaS, SaaS

### Nod

Sicrhau bod cyfrifon defnyddwyr:

- yn cael eu neilltuo i unigolion awdurdodedig yn unig
- ond yn rhoi mynediad at y cymwysiadau, y cyfrifiaduron a'r rhwydweithiau hynny sydd eu hangen ar y defnyddiwr i gyflawni ei rôl

### Cyflwyniad

Mae pob cyfrif defnyddiwr gweithredol yn eich sefydliad yn hwyluso mynediad at ddyfeisiau a chymwysiadau, ac at wybodaeth fusnes sensitif. Drwy wneud yn siŵr mai dim ond unigolion awdurdodedig sydd â chyfrifon defnyddwyr, a'u bod ond yn cael cymaint o fynediad ag sydd ei angen arnynt i gyflawni eu rôl, byddwch yn lleihau'r risg y caiff gwybodaeth ei dwyn neu ei dinistrio.

O gymharu â chyfrifon defnyddwyr arferol, mae gan gyfrifon â breintiau mynediad arbennig fynediad uwch at ddyfeisiau, cymwysiadau a gwybodaeth. Os bydd y cyfrifon hyn dan fygythiad, gallai ymosodwr fanteisio ar eu mynediad uwch er mwyn llygru gwybodaeth ar raddfa fawr, tarfu ar brosesau busnes neu gael mynediad heb awdurdod at ddyfeisiau eraill yn y sefydliad.

Mae gan gyfrifon gweinyddol freintiau arbennig o uchel, er enghraift. Fel arfer, bydd y cyfrifon hyn yn caniatáu i'r defnyddiwr wneud y canlynol:

- gweithredu meddalwedd a all wneud newidiadau sylweddol a newidiadau sy'n gysylltiedig â diogelwch i'r system weithredu
- gwneud newidiadau i'r system weithredu ar gyfer rhai defnyddwyr neu bob un
- creu cyfrifon newydd a dyrannu breintiau

Bydd gan bob math o weinyddwyr y math hwn o gyfrif, gan gynnwys gweinyddwyr part a gweinyddwyr lleol.

Mae hyn yn bwysig oherwydd os bydd defnyddiwr yn agor URL neu atodiad e-bost maleisus, fel arfer byddai'r faleiswedd yn cael ei gweithredu â'r un lefel braint â chyfrif y defnyddiwr. Dyma pam mae'n bwysig bod yn arbennig o ofalus wrth ddyrannu a defnyddio cyfrifon â breintiau.

***Enghraift:** Mae Jody wedi mewngofnodi â chyfrif gweinyddol. Os bydd Jody yn agor URL neu atodiad e-bost maleisus, mae'n debygol y byddai unrhyw faleiswedd cysylltiedig yn cael breintiau gweinyddol. Yn anffodus, dyma'n union beth sy'n digwydd. Gan ddefnyddio breintiau gweinyddol Jody, mae math o faleiswedd a elwir yn feddalweddystlo yn amgryptio'r holl ddata ar y rhwydwaith ac yna'n mynnu pridwerth. Llwyddodd y feddalweddystlo i amgryptio llawer mwy o ddata nag y byddai wedi bod yn bosibl gyda breintiau defnyddiwr safonol, sy'n golygu bod y broblem yn llawer mwy difrifol.*

### Gofynion

Mae'n rhaid i'ch sefydliad reoli eich cyfrifon defnyddwyr a'r breintiau mynediad sy'n caniatáu mynediad at eich data a'ch gwasanaethau sefydliadol. Mae'n bwysig nodi bod hyn hefyd yn cynnwys cyfrifon trydydd parti – er enghraift, cyfrifon a ddefnyddir gan eich gwasanaethau cymorth. Hefyd, mae angen i chi ddeall sut mae cyfrifon defnyddwyr yn dilysu ac yn rheoli'r dull dilysu yn briodol.

Mae hyn yn golygu bod yn rhaid i'ch sefydliad wneud y canlynol:

- sicrhau bod proses ar waith i greu a chymeradwyo cyfrifon defnyddwyr
- dilysu defnyddwyr gan ddefnyddio manylion unigryw cyn rhoi mynediad at gymwysiadau neu ddyfeisiau (gweler dilysu drwy gyfrinair)
- dileu neu analluogi cyfrifon defnyddwyr pan na fydd eu hangen mwyach (er enghraift, pan fydd defnyddiwr yn gadael y sefydliad neu ar ôl cyfnod diffiniedig o anweithgarwch ar y cyfrif)

- rhoi dull dilysu aml-ffactor ar waith, pan fo ar gael – rhaid i brosesau dilysu ar gyfer gwasanaethau cwmwl ddefnyddio dull dilysu aml-ffactor bob amser
- defnyddio cyfrifon ar wahân i gyflawni gweithgareddau gweinyddol yn unig (dim e-bostio, pori ar y we na gweithgareddau defnyddiwr arferol a allai wneud breintiau gweinyddol yn agored i risgiau y gellid eu hosgoi)
- dileu neu analluogi breintiau mynediad arbennig pan na fydd eu hangen mwyach (pan fydd aelod o staff yn newid rôl, er enghraifft)

### Dilysu drwy gyfrinair

Mae'n ofynnol i'r defnyddiwr ddilysu ar gyfer pob cyfrif defnyddiwr.

Pan wneir hyn gan ddefnyddio cyfrinair, dylech roi'r mesurau amddiffynnol canlynol ar waith:

- Caiff cyfrineiriau eu hamddiffyn rhag cael eu dyfalu drwy rym drwy roi o leiaf un o'r canlynol ar waith:
  - proses ddilysu aml-ffactor (gweler isod)
  - cyfyngu ar nifer yr ymgeisiau, fel bod yr amser y mae'n rhaid i'r defnyddiwr aros rhwng ymgeisiau yn cynyddu gyda phob ymgais aflwyddiannus. Ni ddylech ganiatáu mwy na 10 cynnig mewn 5 munud
  - cloi dyfeisiau ar ôl dim mwy na 10 ymgais aflwyddiannus
- Defnyddio rheolaethau technolegol i reoli ansawdd cyfrineiriau. Bydd hyn yn cynnwys un o'r canlynol:
  - Defnyddio dull dilysu aml-ffactor (gweler isod)
  - Sicrhau bod cyfrineiriau yn 12 nod o leiaf, heb gyfyngiad ar yr hyd mwyaf
  - Sicrhau bod cyfrineiriau yn 8 nod o leiaf, heb gyfyngiad ar yr hyd mwyaf ac atal cyfrineiriau cyffredin yn awtomatig gan ddefnyddio rhestr gwrrthod.
- Helpu defnyddwyr i ddewis cyfrineiriau unigryw ar gyfer eu cyfrifon gwaith drwy:
  - addysgu pobl i osgoi defnyddio cyfrineiriau cyffredin, megis enw anifail anwes, patrymau cyffredin ar y bysellwrdd neu gyfrineiriau y maent wedi'u defnyddio yn rhywle arall. Gallai hyn gynnwys addysgu pobl i ddefnyddio'r nodwedd cynhyrchu cyfrinair sydd wedi'i mewnosod ar rai cyfleusterau rheoli cyfrinair.
  - annog pobl i ddewis cyfrineiriau hirach drwy hyrwyddo'r defnydd o sawl gair (o leiaf tri) i greu cyfrinair (megis [canllawiau'r Ganolfan Seiberddiogelwch Genedlaethol ar ddefnyddio tri gair a ddewisir ar hap](#))
  - darparu man storio diogel ar gyfer cyfrineiriau (er enghraifft, cyfleuster rheoli cyfrineiriau neu gwpwrdd diogel dan glo) gyda gwybodaeth glir am sut a phryd y gellir ei ddefnyddio.
  - peidio â gorfodi mesurau sy'n golygu bod cyfrineiriau yn dod i ben
  - peidio â gorfodi gofynion o ran cymhlethdod cyfrineiriau

Dylech hefyd sicrhau bod proses sefydledig ar waith i newid cyfrineiriau yn brydlon os byddwch yn gwybod neu'n amau bod cyfrinair neu gyfrif dan fygythiad

### Dull dilysu aml-ffactor

Yn ogystal â darparu haen ychwanegol o ddiogelwch ar gyfer cyfrineiriau nad ydynt yn cael eu diogelu gan y rheolaethau technegol eraill, dylech bob amser ddefnyddio dull dilysu aml-ffactor er mwyn amddiffyn cyfrifon gweinyddol a chyfrifon sy'n hygrych o'r rhyngrwyd ymhellach.

Rhaid i elfen gyfrinair y dull dilysu aml-ffactor fod yn 8 nod o hyd o leiaf, heb gyfyngiad ar yr hyd mwyaf.

Mae pedwar math o ffactor ychwanegol i'w hystyried:

- dyfais a reolir/sefydliad
- ap ar ddyfais ddibynadwy
- tocyn ffisegol ar wahân
- cyfrif hysbys neu ddibynadwy

Dylid dewis ffactorau ychwanegol fel eu bod yn hygrych a bod modd eu defnyddio. Efallai y bydd angen i chi ymgymryd â phrofion defnyddwyr er mwyn penderfynu beth sydd orau i'ch defnyddwyr. I gael rhagor o wybodaeth, gweler [canllawiau'r Ganolfan Seiberddiogelwch Genedlaethol ar ddilysu aml-ffactor](#).

**Gwybodaeth:** Nid SMS yw'r math mwyaf diogel o ddull dilysu aml-ffactor, ond mae'n cynnig cryn fantais dros beidio â defnyddio dull dilysu aml-ffactor o gwbl. Mae unrhyw ddull dilysu aml-ffactor yn well na pheidio â chael un o gwbl. Fodd bynnag, os oes dulliau amgen ar gael a fydd yn gweithio i'ch sefyllfa, argymhellwn eich bod yn defnyddio'r rhain yn lle SMS.

## 5. Amddiffyn rhag maleiswedd

**Yn gymwys i:** Gweinyddion, cyfrifiaduron bwrdd gwaith, gliniaduron, llechi, ffonau symudol, IaaS, PaaS, SaaS

Nod

Atal maleiswedd hysbys a meddalwedd annibynadwy rhag gweithredu, achosi difrod neu gael gafael ar ddata.

Cyflwyniad

Meddalwedd sy'n cael ei hysgrifennu a'i dosbarthu'n fwriadol i gyflawni gweithredoedd maleisus yw maleiswedd, megis feirybau cyfrifiadurol, mwydod a meddalwedd wyltlo. Mae ffynonellau posibl yn cynnwys: atodiadau maleisus ar negeseuon e-bost, lawrlwythiadau (gan gynnwys rhai o siopau cymwysiadau), a gosod meddalwedd anawdurdodedig yn uniongyrchol.

Os caiff system ei 'heintio', mae'n debyg y bydd eich sefydliad yn dioddef problemau megis systemau yn gwrthod gweithio, colli data, neu haint parhaus a fydd yn anweledig nes y bydd yn achosi niwed yn rhywle arall.

Gallwch osgoi'r posibilrwydd o niwed i raddau helaeth drwy:

- atal maleiswedd rhag cael ei chyflwyno i ddyfeisiau
- atal maleiswedd rhag rhedeg ar ddyfeisiau

**Enghraift:** Mae Acme Corporation yn defnyddio proses llofnodi digidol ochr yn ochr â rheol sy'n golygu mai dim ond cymwysiadau wedi'u fetio o siop gymwysiadau'r ddyfais all weithredu ar y ddyfais. Ni fydd cymwysiadau anghymeradwy a heb eu llofnodi yn rhedeg ar ddyfeisiau. Mae'r ffaith mai dim ond cymwysiadau dibynadwy (sydd ar y rhestr caniatáu) y gall defnyddwyr eu gosod yn golygu bod llai o risg y caiff dyfeisiau eu heintio gan faleiswedd.

Gofynion

Mae'n rhaid i chi sicrhau bod mesur amddiffyn rhag maleiswedd yn weithredol ar bob dyfais o fewn y cwmpas. Ar gyfer pob dyfais, mae'n rhaid i chi ddefnyddio o leiaf un o'r opsiynau a restrir isod. Yn y rhan fwyaf o gynhyrchion modern, bydd yr opsiynau hyn wedi'u cynnwys yn y feddalwedd a ddarperir. Fel arall, gallwch brynu cynhyrchion gan ddarparwr trydydd parti. Ym mhob achos, rhaid

i'r feddalwedd fod yn weithredol, cael ei diweddar yn unol â chyfarwyddiadau'r gwerthwr a'i ffurfweddu i weithio fel y nodir isod:

*Meddalwedd wrthfaleiswedd (opsiwn ar gyfer dyfeisiau o fewn y cwmpas sy'n defnyddio Windows neu MacOS gan gynnwys gweinyddion, cyfrifiaduron a gliniaduron)*

Os byddwch yn defnyddio meddalwedd wrthfaleiswedd i amddiffyn eich dyfais, rhaid ei ffurfweddu fel ei bod yn:

- cael ei diweddar yn unol ag argymhellion y gwerthwr
- atal maleiswedd rhag rhedeg
- atal cod maleisus rhag cael ei weithredu
- atal cysylltiadau â gwefannau maleisus dros y rhyngrywyd

*Rhestr derbyn cymwysiadau (opsiwn ar gyfer pob dyfais o fewn y cwmpas)*

Dim ond cymwysiadau cymeradwy, y cyfyngir arnynt drwy broses llofnodi digidol, y caniateir iddynt weithredu ar ddyfeisiau. Mae'n rhaid i chi:

- gymeradwyo cymwysiadau o'r fath yn fwriadol cyn eu rhoi ar ddyfeisiau
- cynnal rhestr gyfredol o gymwysiadau cymeradwy, ni ddylai defnyddwyr allu gosod unrhyw gymhwysiad nad yw wedi'i lofnodi neu sydd â llofnod annilys.

## D. Canllawiau pellach

### Creu copi wrth gefn o'ch data

Mae creu copi wrth gefn o'ch gwybodaeth yn golygu ei chadw ar ddyfais arall neu ar y cwmwl (ar-lein).

Mae creu copi wrth gefn yn rheolaidd yn golygu y bydd fersiwn ddiweddar o'ch gwybodaeth wedi'i chadw bob amser. Bydd hyn yn eich helpu i adfer yn gynt os bydd eich data'n mynd ar goll neu'n cael eu dwyn.

Gallwch hefyd ddefnyddio proses sy'n creu copiwrth gefn yn awtomatig. Bydd hyn yn cadw eich gwybodaeth ar y cwmwl yn rheolaidd, heb i chi orfod cofio.

Os byddwch yn cadw copi wrth gefn o'ch gwybodaeth ar gof bach USB neu yriant caled allanol, cofiwch ei ddatgysylltu o'ch cyfrifiadur pan na fydd y broses gadw yn mynd rhagddi.

Nid yw creu copi wrth gefn o'ch data yn un o ofynion technegol Cyber Essentials; ond rydym yn argymhell yn gryf eich bod yn defnyddio proses briodol i gadw copiwrth gefn o'ch gwybodaeth.

### Dim Ymddiriedaeth a Cyber Essentials

Mae saerniaeth rhwydweithiau yn newid. Mae mwy o wasanaethau yn symud i'r cwmwl ac mae'r defnydd o Feddalwedd fel Gwasanaeth (SaaS) yn parhau i gynyddu.

Ar yr un pryd, mae llawer o sefydliadau yn croesawu gweithio hyblyg, sy'n golygu y gall llawer o wahanol fathau o ddyfeisiau gysylltu â'ch systemau o sawl lleoliad. Mae hefyd yn dod yn fwyfwy cyffredin i sefydliadau rannu data â'u partneriaid a defnyddwyr gwadd, sy'n golygu bod angen polisiau rheoli mynediad mwy gronynnog.

Mae saerniaeth dim ymddiriedaeth wedi'i dylunio i ymdopi â'r amodau newidiol hyn drwy alluogi profiad gwell i ddefnyddwyr ar gyfer mynediad o bell a rhannu data.

Dull o ddylunio system yw saerniaeth dim ymddiriedaeth lle caiff ymddiriedaeth hanfodol yn y rhwydwaith ei dileu. Yn hytrach, tybir bod y rhwydwaith yn elyniaethus a chaiff pob cais am fynediad ei ddilysu, yn seiliedig ar bolisi mynediad. Ceir hyder mewn cais drwy adeiladu cyd-destun, sy'n dibynnu ar ddilysu cryf, awdurdodi, iechyd y ddyfais, a gwerth y data a gyrchir.

Wrth i sefydliadau symud tuag at fodelau saerniaeth dim ymddiriedaeth, rydym wedi'i ystyried yn y cyd-destun hwn ac yn hyderus nad yw rhoi'r rheolaethau technegol ar waith yn eich atal rhag defnyddio saerniaeth dim ymddiriedaeth fel y'i diffinnir gan [ganllawiau'r Ganolfan Seiberddiogelwch Genedlaethol](#).