

1	<p>Ro-ràdh</p> <p>Tha faclan-faire nam pàirt cudromach de thèarainteachd choimpiutairean agus is iad a’ chiad dìon do chunntasan luchd-cleachdaidh. Dh’fhaodadh facal-faire a chaidh a thaghadh gun aire lìonra Bhòrd na Gàidhlig a chur ann an cunnart. Mar sin tha e an urra ri gach neach-obrach, a’ gabhail a-steach luchd-cùmhnaint is luchd-reice aig a bheil cothrom air siostaman, na ceumannan iomchaidh a ghabhail, mar a thathar a’ mìneachadh gu h-ìseal, gus an cuid fhacal-faire a thaghadh agus a ghleidheadh.</p>	<p>Introduction</p> <p>Passwords are an important aspect of computer security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Bòrd na Gàidhlig network. As such all employees including contractors and vendors with access to systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.</p>
2	<p>Adhbhar</p> <p>Is e adhbhar a’ phoileasaidh seo inbhe a stèidheachadh a thaobh cruthachadh fhacal-faire làidir, dìon nam facal-faire sin, agus cho tric is a thathar gan atharrachadh. Tha am poileasaidh seo mar phàirt de phoileasaidh Bhòrd na Gàidhlig mu rianachd tèarainteachd fiosrachaidh agus mu chleachdadh ceadachte.</p>	<p>Purpose</p> <p>The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. This policy forms part of Bòrd na Gàidhlig information security management and acceptable use policy.</p>
3	<p>Farsaingeachd</p> <p>Tha farsaingeachd a’ phoileasaidh seo a’ bualadh air gach neach-obrach aig a bheil cunntas no ris a bheil cunntas an urra (no cothrom sam bith far a bheil facal-faire comasach no a dhìth) air siostam sam bith ann an ionad sam bith aig Bòrd na Gàidhlig, no aig a bheil cothrom air lìonra Bhòrd na Gàidhlig.</p>	<p>Scope</p> <p>The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Bòrd na Gàidhlig facility or has access to the Bòrd na Gàidhlig network.</p>
4	<p>Aithris mu Phoileasaidh</p> <p>Faid Fhacal-faire air a’ Char as Lugha</p> <p>Anns gach facal-faire aig ìre luchd-cleachdaidh (mar eisimpleir, cunntas neach-cleachdaidh) bidh 10 caractaran air a’ char as lugha le measgachadh àireamhan is litrichean agus de caractaran sònraichte; mura bheil facal-faire deich caractaran comasach ann an siostam sònraichte, thèid an àireamh as motha de caractaran a cheadaichear leis an t-siostam sin a chleachdadh.</p>	<p>Policy Statement</p> <p>Minimum Password Length</p> <p>All user-level passwords (e.g. user account) shall have a minimum of ten characters with a mix of alphanumeric and special characters; if a particular system will not support ten-character passwords, then the maximum number of characters allowed by that system shall be used.</p>

Feumaidh co-dhiù 20 caractar a bhith anns gach facal-faire aig ìre an t-siostaim saothrachaidh (m.e. faclan-faire root, comasachaidh, rianairean àrainnean is msaa). Anns gach facal-faire aig ìre siostam-riochdachaidh (mar eisimpleir freumh, comasaich, luchd-rianachd àrainnean agus an leithid) bidh fichead caractar air a' char as lugha; mura bheil facal-faire fichead caractar comasach ann an siostam sònraichte, thèid an àireamh as motha de characteran a cheadaichear leis an t-siostam sin a chleachdadh.

Cruthachadh Fhacal-faire

Cha tèid faclan-faire a chruthachadh ann am facal no faclan faclair ann an cànan sam bith. Cha tèid faclan-faire a dhèanamh suas le fiosrachadh-sònrachaidh a tha aithnichte no air a phostadh gu poblach.

BitLocker

Tha tuilleadh dìon air laptopan agus coimpiutairean Bhòrd na Gàidhlig le crioptachadh BitLocker. Tha seo ag iarraidh air luchd-cleachdaidh còd PIN a chruthachadh a dh' fheumar a chuir a-steach gus an draibhear fhuasgladh, mus cuir iad a-steach facal-faire an t-siostaim.

5 Modh-obrach

Tasgadh Fhacal-faire

Nuair a dh'fheumar facal-faire a sgrìobhadh sìos air adhbharan tuiteamais (mar eisimpleir faclan-faire putaidh agus faclan-faire luchd-rianachd) bu chòir an cur ann an cèis-litreach air a seulachadh agus an cur ann an ciste-thasgaidh dìonach bho theine.

Cha sgrìobh ann an suidheachadh sam bith luchd-cleachdaidh an cuid fhacal-faire sìos no an nochdadh ri luchd-cleachdaidh eile. Feumar a h-uile coimeasgachadh de dh'ainmean-chleachdaichean/de dh'fhaclan-faire aig ìre siostam-

All production system-level passwords (e.g. root, enable, domain administrators, etc) shall have a minimum of twenty characters; if a particular system will not support twenty-character passwords, then the maximum number of characters allowed by that system shall be used.

Password Composition

Passwords shall not be composed of one or more dictionary words in any language. Passwords shall not consist of well-known or publicly posted identification information

BitLocker

All Bòrd na Gàidhlig laptops and PCs are further protected by BitLocker encryption. This requires users to create a PIN code that must be entered to unlock the drive, prior to entering the system password.

Procedure

Password Storage

Where it is necessary to write down a password for contingency reasons (e.g. boot passwords and administrator passwords), they should be put in a sealed envelope and placed in a fireproof safe.

Under no circumstances shall users write down their passwords or share them with other users. All production system-level username/password combinations must be recorded in a secure password manager.

riochdachaidh a chlàradh ann an rianadair tèarainte do dh'fhaclan-faire.

Cha bu chòir gun tèid faclan-faire a chuimhneachadh le prògraman-coimpiutair gun chrioptachadh leithid post-dealain. Gabhar ri cleachdadh prògram-tasgaidh fhacal-faire gun chrioptachadh, ach feumar aire mhath a ghabhail gus casg a chur air cothrom air a' phrògram sin.

Faclan-faire a' Fàs Sean

Chan eil crìochnachadh fhacal-faire a' bualadh air faclan-faire ìre luchd-cleachdaidh (mar eisimpleir, post-dealain, coimpiutair-deasg, lìon agus an leithid) ach feumar an atharrachadh ma shònraichear no ma nochdar teagamh mu bhriseadh a-steach.

Ath-chleachdadh Fhacal-faire

Thèid aire a ghabhail gus nach cuirear an tèarainteachd aig iomadh shiostaman no ghoireasan goireas iomadach ann an cunnart fhad is a chleachdar an aon ainm-cleachdaiche no an aon fhacal-faire gus cothrom fhaighinn. Tha seo na stiùireadh do luchd-obrach/luchd-cleachdaidh nach bu chòir do neach na h-aon fhaclan-faire air an aon rèir a chleachdadh ann an diofar shiostaman. Ma bhrisear a-steach air an fhacal-faire, tha an cunnart don tèarainteachd gu math farsaing.

Tar-chur Dealantach

Cha tèid faclan-faire a chur a-null gu dealantach tron Eadar-lìon a' cleachdadh mhodhan gun tèarainteachd. Cha tèid ach pròtacalan tèarainte, HTTPS, FTPS, agus an leithid nam measg, a chleachdadh.

Dubhadh às Fhacal-faire

Feumar gach facal-faire nach eil a dhìth tuilleadh a dhubhadh às no a chur bho chomas gun dàil. Tha seo a' gabhail a-

Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.

Password Aging

User-level passwords (e.g. email, desktop computer, web, etc.) are not subject to a password expiry however must be changed on indication or suspicion of compromise.

Password Reuse

Care shall be taken to prevent the compromise on the security of multiple systems or resources while using the same username and password for access. This is a guideline to staff/users that one should not use the same matching passwords in various systems. If the password is compromised, the security compromise is extensive.

Electronic Transmission

Passwords shall not be transferred electronically over the Internet using insecure methods. Only secure protocols including HTTPS, FTPS, etc shall be used.

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

steach na leanas, ach gun a bhith cuibhrichte riutha:

- Nuair a leigeas neach-cleachdaidh a dhreuchd bhuaithe, nuair a thèid a chur gu dreuchd eile, a leigeil mu sgaoil, a chur à dreuchd agus an leithid
- Thèid faclan-faire bunailteach atharrachadh gun dàil air gach uidheam
- Cunntasan luchd-cùmhnaint nuair nach fheum iad an cuid dhleastanasan a choileanadh tuilleadh
- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment
- Contractor accounts, when no longer needed to perform their duties

Nuair nach eil facl-faire a dhìth tuilleadh, bu chòir na modhan-obrach a leanas a leantainn:

- Bu chòir dhan neach-obrach fios a leigeil dhan neach-stiùiridh aige
- Bu chòir do neach-cùmhnaint fios a leigeil dhan neach-chonaltraidh aige
- Bu chòir dhan neach-stiùiridh no dhan neach-chonaltraidh fios a leigeil dhan deasg-chuideachaidh (support@microtech-group.co.uk) no an t-atharrachadh a tha a dhìth a dhèanamh, agus nuair a tha e iomchaidh, an cunntas nach eil a dhìth tuilleadh a chur bho chomas/a dhubhadh às
- When a password is no longer needed the following procedures should be followed:
- Employee should notify his or her immediate supervisor
- Contractor should inform his or her point of contact
- Supervisor or point of contact should either notify the help desk (support@microtech-group.co.uk) or make the necessary change, and where appropriate disable/delete redundant account

6 Feumalachdan airson Luchd-rianachd Shìostaman

Requirements for System Administrators

Faclan-faire a dhìth airson Logadh a-steach

Require Passwords for Login

Cha tèid sìostaman a cho-dhealbhachadh rèiteachadh gus logadh a-steach le cleachdaiche a cheadachadh gun fhacal-faire.

Systems shall not be configured to allow user login without a password.

Dion an Aghaidh Hacaigeadh Fhacal-faire

Protect Against Password Hacking

Nì luchd-rianachd shiostaman an cuid shiostaman a dhèanamh nas cruaidhe gus briseadh a-steach air faclan-faire a bhacadh le bhith a' cleachdadh mhodhan reusanta gus ionnsaighean borb air faclan-faire a lasachadh. Mar eisimpleir, glasaiddh cuid de shiostaman cunntas fad beagan mhionaidean an dèidh caochladh oidhirpean air logadh a-steach a dh'fhairtlich, no lorgaidh iad cò às a tha an ionnsaigh a' tighinn agus barrachd ionnsaighean bhon àite sin a bhacadh.

Ag Atharrachadh Fhacal-Faire an Dèidh Briseadh A-Steach no Nochdadh

Cuiridh luchd-rianachd shiostaman, cho luath is a ghabhas, faclan-faire ùra ri cunntasan luchd-cleachdaidh no iarraidh iad air luchd-cleachdaidh na faclan-faire aca a shuidheachadh às ùr ann an suidheachaidhean far an cruthaich cleachdadh leanmhainneach de dh'fhacal-faire cunnart gum faighear cothrom gun ùghdarrachadh air a' chunntas no air a' ghoireas-choimpiutaireachd. Am measg eisimpleirean de na suidheachaidhean seo, cho math ri suidheachaidhean eile, tha nochdadh facail-fhaire ri neach gun ùghdarrachadh; lorg facail-fhaire le neach gun ùghdarrachadh; briseadh a-steach air siostam no cunntas gun ùghdarras; facal-faire ga chur a-null gun tèarainteachd; a' cur an àite cleachdaiche cunntais neach eile a tha feumach air cothrom air an aon chunntas; facal-faire ga thoirt do luchd-obrach IT gus ceist theicnigeach fhuasgladh; facal-faire cunntais ga chonaltradh gu cleachdaiche le rianadair an t-siostaim. Cuideachd, aon uair is gun tèid am facal-faire a shuidheachadh às ùr, feumaidh an neach-cleachdaidh am facal-faire ùrachadh aig an ath logadh a-steach a nì e.

Faclan-faire Bunailteach

Cha chleachd luchd-rianachd shiostaman faclan-faire bunailteach airson cunntasan-rianachd.

System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate brute force password attacks. For example, some systems will lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts from that location.

Changing Passwords After Compromise or Disclosure

System administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorised access to the computing account or resource. Examples of these situations include, but are not limited to, disclosure of a password to an unauthorised person; discovery of a password by unauthorised person; system compromise (unauthorised access to a system or account); insecure transmission of a password; replacing the user of an account with another individual requiring access to the same account; password is provided to IT Staff in order to resolve a technical issue; account password is communicated to a user by the system administrator. Also, once the password is reset, the user is forced to change password at next logon.

Default Passwords

System administrators shall not use default passwords for administrative accounts.

7 Pàipearan-taic

Stiùireadh mu Chruthachadh Fhacal-faire

Modhan ris an Gabhar gus facal-faire làidir a chruthachadh

- Cleachd 10 caractaran air a' char as lugha. Anns an fharsaingeachd, mar as motha de caractaran a chleachdas tu, is ann as doirbhe a tha e facal-faire a bhriseadh no a thomhas
- Cleachd measgachadh de litrichean beag is mòra
- Cleachd caractaran sònraichte agus samhlaidhean-puingeachaidh (m. e. `+!@%*&".:/`)

Modhan ris Nach Gabhar gus Facal-Faire Làidir a'Chruthachadh

- Na cleachd faclan à faclair, Chan eil faclan nach eil nam faclan Beurla càil sam bith nas tèarainte na faclan a tha nam faclan Beurla
- Na cleachd faclan, àireamhan, no fiosrachadh air a bheil am poball eòlach ceangailte riut (m. e. Ainmean, ainmean an teaghlach, làithean-breith, àireamhan-fòn agus an leithid
- Na cleachd d' ainm logadh a-steach no dreach sam bith de d' ainm logadh a-steach mar am facal-faire agad
- Na cleachd an caractar ceudna airson an fhacail-fhaire air fad (m. e. 111111) agus na cleachd nas lugha na 5 caractaran air leth.
- Na cleachd pàtranan cumanta de litrichean no de dh'àireamhan anns an fhacal-fhaire agad (m. e. 123456 no abcdefgh)
- Cha bu chòir ionadachadh a chleachdadh air faclan cumanta no le

Appendices

Guidelines on Password Creation

Acceptable Methods to create a strong password

- Use a minimum of 10 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed
- Use mixed case (upper & lower)
- Use special characters and punctuation symbols (e.g. `+!@%*&".:/`)

Unacceptable Methods to Create a Strong Password

- Do not use dictionary or actual words. Non-English words are no more secure than English words
- Do not use words, numbers, or known or public information associated with you (e.g. Names, family names, pet names, birthdays, phone numbers etc
- Do not use your login name or any variation of your login name as your password
- Do not use the same character for the entire password (e.g. 111111) or use fewer than 5 unique characters.
- Do not use common letter or number patterns in your password (e.g. 123456 or abcdefgh)
- Substitution should not be used on common words or with common substitutions (e.g. 3=E, 4=A, 1=l, 0=O, etc.)

ionadachaidhean cumanta (m. e. 3=E, 4=A, 1=I, 0=O, agus mar sin air adhart)

- Nuair a bhios facal-faire ga atharrachadh, atharraich e gu facal-faire a tha gu tur ùr. Na rach mun cuairt liosta de na faclan-faire as fheàrr leat, agus na h-atharraich dìreach aon character (m.e. P4sswOrd1, P4sswOrd2, P4sswOrd3, agus mar sin air adhart)
- When changing a password, change to an entirely new password. Do not just rotate through a list of favourite passwords, or alternate a single character (e.g. P4sswOrd1, P4sswOrd2, P4sswOrd3, etc)

Feumalachdan fhacal-faire

Tha na feumalachdan fhacal-faire a leanas gan socrachadh le Tèarainteachd IT:

- Faid as Giorra – 10 caractaran gam moladh
- Faid as Fhaide – Chan eil faid as fhaide ga moladh
- Toinnteachd as lugha – Gun fhaclan à faclair ann. Bu chòir gun cleachdadh faclan-faire a h-uile gin de na ceithir seòrsaichean caractaran a leanas:
 - Litrichean beaga
 - Litrichean mòra
 - Àireamhan
 - Caractaran sònraichte leithid +=!@%*&".:/
- Tha faclan-faire a' toirt aire do mhòr seach beag agus chan eil an t-ainm-cleachdaiche no an ID gus logadh a-steach a' toirt aire do mhòr seach beag
- Eachdraidh fhacal-faire – cùm cuimhne air 5 faclan-faire a bha agad
- Aois fhacal-faire – chan eil crìochnachadh air cunntasan luchd-cleachdaidh
- An ìre as motha ro ghlasadh a-mach – 5 oidhirpean air logadh a-steach a dh'fhairtlich.

Password requirements

The following password requirements are set by IT Security:

- Minimum Length – 10 characters recommended
- Maximum Length – No maximum length recommended
- Minimum complexity – No dictionary words included. Passwords should use all four of the following types of characters:
 - Lowercase
 - Uppercase
 - Numbers
 - Special characters such as +=!@%*&".:/
- Passwords are case sensitive and the username or login ID is not case sensitive
- Password history – remember 5 old passwords
- Password age – no expiry on user accounts
- Account lockout threshold – 5 failed login attempts

8 Cur an Gnìomh

Faodar smachdachadh a chur air neach-obrach a bhris am poileasaidh, às am faodadh crìoch air fastadh tighinn, an crochadh air cho dona agus a tha am briseadh. Faodaidh briseadh a' phoileasaidh seo le neach-obrach sealach, neach-cùmhnant no neach-reic crìoch air a' chùmhntant no air an dleastanas aca le Bòrd na Gàidhlig adhbharachadh.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action and may include termination of employment depending on the severity of the violation. A violation of this policy by a temporary worker, contractor or vendor may result in termination of their contract or assignment with Bòrd na Gàidhlig.

9 Measadh na Buaidhe air Co-ionannachd

Tha Bòrd na Gàidhlig ag aithneachadh a dhleastanas a bhith a' dèanamh cinnteach nach eil leth-bhreith no ana-cothrom air duine air sgàth aois, ciorram, ath-shònrachadh gnè, pòsadh agus com-pàirteachas catharra, leatromachd agus màthaireachd, cinneadh, creideamh no feallsanachd, gnè no taobhadh feise.

Equality Impact Assessment

Bòrd na Gàidhlig recognises its responsibility to ensure that no-one is discriminated against or disadvantaged on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation.

10 Faclair

Eachdraidh Fhacal-faire – Àireamh nam faclan-faire ùra air leth a dh'fheumas a bhith ceangailte ri cunntas neach-cleachdaidh mus fhaodar facal-faire aosta a chleachdadh a-rithist. Feumaidh a luach a bhith eadar 0 agus 24 de dh'fhaclan-faire.

Glossary

Password History – The number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.

Caractaran Sònraichte – Caractaran air a' chlàr-iuchraichean nach eil nan litir seach nan àireamh a dh'fhaodar cleachdadh gus toinnteachd fhacal-faire a mheudachadh.

Special Characters – Characters on the keyboard that do not do not fall under alphanumeric moniker that can be used to increase password complexity

Hacaigeadh – Oidhirpean gun ùghdarrachadh air cothrom fhaotainn air goireasan Bhòrd na Gàidhlig.

Hacking – Unauthorised attempts to gain access to Bòrd na Gàidhlig resources.

11 Smachd Sgrìobhainn**Document Control**

Dreach <i>Version Number</i>	Adhbhar/Atharrachadh <i>Purpose/Change</i>	Ùghdar <i>Author</i>	Ceann-là <i>Date</i>



Poileasaidh Teàrainteachd Dhidseatach
Cyber Resilience Policy

Air aontachadh le/Approved by:

Air aontachadh air/Approved on:

Ath-nuadhachadh a dhìth/Review due on:

Eadar-theangachadh dearbhte/translation checked:

	Clàr-Innse	Index	Duilleag /Page
1	Ro-ràdh	Introduction	3
2	Adhbhar	Purpose	3
3	Farsaingeachd	Scope	3
4	Aithris Poileasaidh	Policy Statement	3
5	Modh-obrach Rianachd Ghàbhaidhean Didseatach Sgrùdadh air Gàbhadh Didseatach	Procedure Cyber Risk Management Cyber Risk Analysis	4
7	Pàipearan-taic Poileasaidhean-taic	Appendices Supporting Policies	5
8	Cur an Gnìomh	Enforcement	6
9	Faclair	Glossary	6
10	Smachd Sgrìobhainn	Document Control	

1 Ro-ràdh

Tha Bòrd na Gàidhlig air cumail ri Plana-gnìomha na Roinne Poblach (PSAP) air Tèarainteachd Dhìseatach a chaidh a chur air bhog air 8 Samhain 2017 leis an Leas-phrìomh Mhinistear agus a chaidh a chruthachadh ann an com-pàirteachas le Riaghaltas na h-Alba agus Bòrd nan Ceannardan Teàrainteachd Dhìseatach (*National Cyber Resilience Leaders Board* - NCRLB). Tha am Plana-gnìomha a' nochdadh nan gnìomhan bunaiteach a ghabhas Riaghaltas na h-Alba, is e ag obair gu dlùth leis an NCRLB, le buidhnean poblach agus com-pàirtichean bunaiteach gu deireadh 2018 gus tèarainteachd dhìseatach ann an roinn phoblach na h-Alba a mheudachadh barrachd.

2 Adhbhar

Is e adhbhar a' phoileasaidh seo seòladh a stèidheachadh gus am bi Bòrd na Gàidhlig air an aon rèir ri poileasaidh Riaghaltas na h-Alba mu Thèarainteachd Dhìseatach, gus neartan agus/no laigsean a shònrachadh, gus ro-innleachd làidir mu Thèarainteachd Dhìseatach a chruthachadh is a ghleidheadh gu sònraichte, a' lasachadh ghàbhaidhean ag èirigh an-dràsta agus san ùine air thoiseach.

3 Farsaingeachd

Thathar air am poileasaidh seo a chruthachadh ann an oidhirp cumail ri plana-gnìomha tèarainteachd dhìseatach a tha a' bualadh air gach buidheann phoblach, Bòrd na Gàidhlig nam measg. Tha am poileasaidh seo a' bualadh air nì sam bith a dh'fhaodadh bagairt air Bòrd na Gàidhlig air an taobh a-muigh no an taobh a-staigh.

4 Aithris mu Phoileasaidh

Agus eucoir dhìseatach na ceist mhòr do gach gnìomhachas ceangailte ris an Eadar-lìon agus le atharrachadh o chionn ghoirid air reachdas Eòrpach ag adhbharachadh dòigh-dèiligidh throm gus oidhirp nas cùramaiche a chur an gnìomh gus èifeachdalachd innleachdan tèarainteachd dhìseatach anns an fharsaingeachd a leasachadh, tha Riaghaltas na h-Alba air Frèam Tèarainteachd Dhìseatach na Roinne Phoblach a chur ri chèile.

Introduction

Bòrd na Gàidhlig has followed the Public Sector Action Plan (PSAP) on Cyber Resilience launched on 8 November 2017 by the Deputy First Minister and developed in partnership by the Scottish Government and the National Cyber Resilience Leaders Board (NCRLB). The Action Plan set out the key actions that the Scottish Government, working closely with the NCRLB, public bodies and key partners will take up to the end of 2018 to further enhance cyber resilience in Scotland's public sector.

Purpose

The purpose of this policy is to establish a roadmap for Bòrd na Gàidhlig to remain in lock-step with Scottish government Cyber Resilience policy, identify areas of strength and/or weakness, to specifically develop and maintain robust Cyber Security strategy mitigating emerging and future threats.

Scope

This policy has been created to adhere to cyber resilience action plan applying to all public bodies including Bòrd na Gàidhlig. This policy applies to all or any facet that presents exposure and risk to Bòrd na Gàidhlig from external or internal sources

Policy Statement

With cyber crime a primary concern for all internet connected business and with recent change in European legislation driving an onerous approach to enforce a more responsible effort to improve general effectiveness of cyber resilience mechanisms. Scottish Government has developed the Scottish Public Sector Cyber Resilience Framework.

Feumaidh Bòrd na Gàidhlig mar sin ceuman a mhìnichear ann an clàr PSAP a chur an sàs agus obrachadh le Riaghaltas na h-Alba gus na clàran-ama a tha a dhìth a choileanadh. Air an ainmeachadh gu h-ìosal tha na feumalachdan bunaiteach air an feum Bòrd na Gàidhlig aghaidh a chur agus a ghleidheadh gus a dhearbhadh gu bheil a' cumail ri poileasaidh Riaghaltas na h-Alba, ùrachadh air leasachaidhean mu dhìon an aghaidh bhagairtean san ùine air thoiseach nam measg.

It is therefore mandatory for Bòrd na Gàidhlig to put in place measures as outlined in the PSAP implementation toolkit demonstrating ability to respond timely and work collaboratively with SG to meet required timescales. Listed below are the key requirements Bòrd na Gàidhlig needs to address and maintain to ensure lock-step compliance with SG policy including update amendment encompassing future threat protection.

- Gèilleadh ri Frèam Tèarainteachd Dhìseatach na Roinne Phoblach
- Riaghladh (Cuir ball den Bhòrd/Luchd-stiùiridh an dreuchd ris am bi Tèarainteachd Dhìseatach an urra)
- Ballrachd CiSP
- Dearbhadh neo-eisimeileach iomchaidh mu smachdan bunaiteach (teisteanas ann an Didseatachd Bhunaiteach)
- Ceuman dìon didseatach an gnìomh (Seirbheis DNS Roinn Phoblach na RA, DMARC, anti-spoofing, Webcheck, Netcraft)
- Trèanadh is ullachadh luchd-obrach
- Gnìomhan fhreagairtean air tachartasan air an toirt a-steach do phlana leantainneachd gnìomhachais
- Compliance with Scottish Public Sector Cyber Resilience Framework
- Governance (Appoint Board/Senior Management member responsible for Cyber Resilience)
- CiSP membership
- Appropriate independent assurance of critical controls (Cyber Essentials Plus certification)
- Active cyber defence measures (UK Public Sector DNS service, DMARC, anti-spoofing, Webcheck, Netcraft)
- Staff training and awareness raising
- Incident response procedures included in business continuity plan

5 Modh-obrach

Procedure

Rianachd Ghàbhaidhean Didseatach

Cyber Risk Management

Tha measadh ghàbhaidhean didseatach ga mhìneachadh mar shònrachadh, sgrùdadh agus measadh ghàbhaidhean didseatach. Bidh e a' sgrùdadh is a' measadh bun-structar IT uile agus a' comharrachadh laigsean a dh'fhaodadh èirigh far a bheil daoine, modhan-obrach is teicneòlas a' tighinn còmhla, cho math ri laigsean anns na diofar shiostaman.

Cyber risk assessment is defined as the identification, analysis and evaluation of cyber risks. It studies and analyses the entire IT infrastructure and identifies possible vulnerabilities at the juncture of people, processes and technology, as well as vulnerabilities within the different systems.

An dèidh dhan aonta a bhith air a dèanamh, is e rianachd ghàbhaidhean an ath cheum

After the assessment has been made, the next logical step is risk

loidigeach. Bidh prògram rianachd ghàbhaidhean mar sin a' toirt prìomhachas do na gàbhaidhean a shònraichear a thaobh cho coltach is a tha e gun èireadh iad, agus a' dèanamh oidhirpean air an co-òrdanachadh an dèidh sin gus buaidh nan gàbhaidhean sin a chumail aig an ìre as lugha, a dhearcnachadh agus a riaghladh.

Tha gàbhadh didseatach ga mhìneachadh mar thachartas sam bith às an tigeadh briseadh dàta, call ionmhasail, milleadh air cliù, agus briseadh a-steach air obrachaidhean air adhbharachadh le faireachadh air siostaman is modhan-obrach teicneòlais.

Gabh ri dòigh-dèiligidh cearcaill-bheatha mu rianachd ghàbhaidhean: Bidh teicneòlas ag atharrachadh, mar a bhios agus am bagairt agus a rèir sin bidh gàbhaidhean ag atharrachadh tro thìde. Feumar gabhail ri dòigh-dèiligidh modh-obrach fad-beatha leanmhainneach gus a dhearbhadh gum bi riaghladh air tèarainteachd èifeachdach is iomchaidh fad na tìde.

Brosnaich cleachdaidhean rianachd ghàbhaidhean: Feumaidh rianachd ghàbhaidhean a bhith ann air feadh na buidhne, air a stiùireadh le luchd-stiùiridh Bhòrd na Gàidhlig bhon bhàrr a-nuas, le com-pàirteachais luchd-cleachdaidh ga nochdadh aig gach ìre den ghnìomhachas.

Sgrùdadh air Gàbhadh Didseatach

Tha Bòrd na Gàidhlig air barantas Cyber Essentials Plus fhaighinn agus thathas airson seo a chumail.

Thèid breithneachadh às ùr air ceuman a bharrachd agus thèid an cur ris na gnìomhan againn mu Thèarainteachd Dhidseatach.

management. Thus, a cyber risk management programme prioritises the identified risks in terms of likelihood of occurrence, then makes coordinated efforts to minimise, monitor and control the impact of those risks.

Cyber risk is defined as any event that can lead to data breaches, financial loss, reputational damage, and disruption of operations caused by a failure of technology systems and procedures.

Adopt a lifecycle approach to risk management: Technology changes, as does the threat and therefore risks change over time. A continuous through-life process needs to be adopted to ensure security controls remain effective and appropriate.

Promote a risk management culture: Risk management needs to be organisation-wide, driven by Bòrd na Gàidhlig senior management from the top down, with user participation demonstrated at every level of the business.

Cyber Risk Analysis

Bòrd na Gàidhlig has achieved Cyber Essentials Plus certification and is committed to maintaining this.

Further measures will be reviewed and added to our cyber resilience response.

6 Poileasaidhean-taice

Ro-innleachd ICT

Poileasaidh mu Chleachdadh ris an Gabhar

Poileasaidh Fhacal-faire

Poileasaidh nam Meadhanan Sòisealta

Plana Leantainneachd Gnìomhachais

Supporting Policies

ICT Strategy

Acceptable Use Policy

Password Policy

Social Media Policy

Business Continuity Plan

7 Cur an Gnìomh

Chan fhaodar goireasan Bhòrd na Gàidhlig a chleachdadh air adhbhar sam bith a tha mì-laghail no toirmisgte a rèir poileasaidhean, inbhean agus treòrachadh Bhòrd na Gàidhlig. Feumar fios a thoirt do luchd-obrach Bhòrd na Gàidhlig mu na poileasaidhean seo, na gàbhaidhean ceangailte ri eucoir dhidseatach agus feumar fios a chumail riutha mu na modhan gus brath a ghabhail agus iad ag atharrachadh fad na tìde. Tha tèarainteachd is cleachdadh iomchaidh ghoireasan lìonra Bhòrd na Gàidhlig a tha fo smachd aca an urra ris an luchd-obrach agus cuideachd a bhith cùramach is mothachail air gnìomhan no ionnsaighean mu bheil amharas agus an t-amharas sin a chur an cèill dhan luchd-stiùiridh aca.

Is e uallach coitcheann a tha ann an casg air Eucoir Dhidseatach, bu chòir gum biodh gach neach-obrach mothachail air buaidhean agus cho trom agus a tha brisidhean, agus chan eil aineolas na leisgeul idir. Faodaidh gun tèid smachdachadh a chur air luchd-obrach a nì dearmad follaiseach, gu ìre crìoch a chur air fastadh. Faodaidh gun tig mar thoradh air briseadh air a' phoileasaidh seo le neach-obrach sealach, neach-cùmhnaint no neach-reic crìoch air a' chùmhnant no an dleastanas aca le Bòrd na Gàidhlig.

8 Faclair

Eucoir Dhidseatach – Eucoir ag amas air àrainneachdan-coimpiutaireachd agus tèarainteachd a bhriseadh no cothrom dligheach a chur an cunnart.

Com-pàirteachas Roinneadh Fios mu Thèarainteachd Dhidseatach/Cyber Security Information Sharing Partnership (CiSP)

Ionad Nàiseanta Tèarainteachd Dhidseatach/National Cyber Security Centre (NCSC)

Plana-gnìomha na Roinne Phoblach/Public Sector Action Plan (PSAP)

Solaraiche Sheirbheisean air an Rianachd/Managed Service Provider (MSP)

Enforcement

Bòrd na Gàidhlig resources may not be used for any unlawful or prohibited purpose in accordance with Bòrd na Gàidhlig policies, standards, and guidelines. Bòrd na Gàidhlig employees must be made aware of these policies, risks posed by cybercrime and kept up to date with the ever-changing exploitation methods. Employees are responsible for the security and appropriate use of Bòrd na Gàidhlig network resources under their control and to remain vigilant and mindful of suspicious activity or attack. Reporting all such suspicion to their line manager.

Cybercrime prevention is a shared responsibility, all employees should be aware of consequences and alert of the seriousness of breach, ignorance is no excuse. Employees found blatantly negligent, careless or malicious in this regard may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Bòrd na Gàidhlig.

Glossary

Cybercrime – Criminal activity aimed at computerised environments designed to breach security or compromise legitimate access.

Cyber Security Information Sharing Partnership (CiSP)

National Cyber Security Centre (NCSC)

Public Sector Action Plan (PSAP)

Managed Service Provider (MSP)

9 Smachd Sgrìobhainn

Document Control

Dreach <i>Version Number</i>	Adhbhar/Atharrachadh <i>Purpose/Change</i>	Ùghdar <i>Author</i>	Ceann-là <i>Date</i>



Poileasaidh Smachd air Inntrigeadh
Access Control Policy

Air aontachadh le/Approved by:

Air aontachadh air/Approved on:

Ath-nuadhachadh a dhith/Review due on:

Eadar-theangachadh dearbhte:

	Clàr-Innse	Index	Duilleag /Page
1	Ro-ràdh	Introduction	3
2	Adhbhar	Purpose	3
3	Farsaingeachd	Scope	3
3	Aithris Poileasaidh	Policy Statement	3
4	Pròiseas	Process	4
5	Cur an Gníomh	Enforcement	8
6	Measadh na Buaidhe air Co- ionannachd	Equality Impact Assessment	9
7	Smachd Sgrìobhainn	Document Control	9

1 Ro-ràdh

Tha fiosrachadh na stòras cudromach agus luachmhor airson seirbheisean Bhòrd na Gàidhlig agus feumar dìon agus smachd ceart a bhith air. Chaidh smachdan inntigidh rangachail a chruthachadh leis an sgioba stiùiridh agus chaidh an cur an gnìomh air feadh na buidhne gus fiosrachadh agus dàta a dhìon bho inntrigeadh gun chead.

Introduction

Information is an important and valuable asset to Bòrd na Gàidhlig services and requires accurate protection and control. Hierarchical access controls have been developed by the management team and implemented throughout the organisation to safeguard information and data from unauthorised access.

2 Adhbhar

Tha smachdan air inntrigeadh an sàs gus fiosrachadh a dhìon le bhith a' cumail smachd air cò aig a bheil na còraichean gus diofar ghoireasan fiosrachaidh a chleachdadh agus le bhith gan dìon an aghaidh cleachdadh gun chead. 'S e adhbhar a' phoileasaidh seo dèanamh cinnteach gum bi smachd air inntrigeadh air fiosrachadh is siostaman agus gu bheil dòighean-obrach ann gus dèanamh cinnteach gun tèid siostaman agus dàta a dhìon.

Purpose

Access controls are in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use. The purpose of this policy is to ensure access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

3 Farsaingeachd

Tha am poileasaidh seo an sàs airson buill agus luchd-obrach, cunnadairean, comhairlichean agus luchd-obrach sealach uile agus feumaidh daoine eile, a' gabhail a-steach an luchd-obrach uile aig treas-phàrtaidhean a tha ag obair às leth Bòrd na Gàidhlig am poileasaidh seo a leantainn. Tha am poileasaidh seo a' buntainn ri stòrasan fiosrachaidh le Bòrd na Gàidhlig no a tha aig a' Bhòrd air mhàl, agus ri innealan no seirbheisean a nì ceangal ri lìonra Bhòrd na Gàidhlig, no a tha a' stèidhichte ann an oifisean Bhòrd na Gàidhlig.

Scope

This policy applies to all members and employees, contractors, consultants, temporary and other individuals, including all personnel affiliated with third parties working on behalf of Bòrd na Gàidhlig, must adhere to this policy. This policy applies to information assets owned or leased by Bòrd na Gàidhlig, or to devices or services that connect to a Bòrd na Gàidhlig network or reside at Bòrd na Gàidhlig premises.

4 Aithris Poileasaidh

Tha dleastanas laghail air Bòrd na Gàidhlig dèanamh cinnteach gu bheil am fiosrachadh uile a bhios e a' pròiseasadh às leth nan daoine is luchd-ùidh aige sàbhailte agus dìomhair.

Policy Statement

Bòrd na Gàidhlig is legally required to ensure the security and confidentiality of the information it processes on behalf of its people and stakeholders.

Tha Bòrd na Gàidhlig airson 's gum bi smachdan air inntrigeadh air an cleachdadh agus air an stiùireadh gu ceart air feadh na buidhne. Ma tha dìth smachd air inntrigeadh, no ma tha inntrigeadh ann gun bhacadh sam bith air, dh'fhaodadh gun rachadh fiosrachadh a ghoid no fhoillseachadh gun ùghdarras agus gum faodadh foill a bhith ann agus gum faodadh cùisean laghail a bhith ann mar thoradh air seo. 'S e adhbhar a' phoileasaidh a bhith a' mìneachadh cleachdadh ceart agus a' mìneachadh nan smachdan inntrigidh aig an luchd-stiùiridh taobh a-staigh Bòrd na Gàidhlig.

Bòrd na Gàidhlig is committed to the correct use and management of access controls throughout the organisation. Insufficient access controls or unmanaged access to information could lead to the unauthorised disclosure or theft of this information, fraud and possible litigation. The purpose of this policy is to define the correct use and management access controls within Bòrd na Gàidhlig.

5 Pròiseas

Process

Cleachdaichean Ùra

New Users

Thèid ID cleachdaiche sònraichte a thoirt do gach neach-cleachdaidh taobh a-staigh Bòrd na Gàidhlig gus inntrigeadh a thoirt dhaibh do shiostaman-obrachaidh a tha air an cleachdadh airson cruthachadh, sgaoileadh agus stòradh fiosrachaidh. Nì an ID air leth seo cinnteach gun gabh cleachdaichean a cheangail ri, agus a bhith air an cumail cunntachail airson, an cuid ghnìomhan nuair a tha iad ag inntrigeadh fiosrachadh. Chan eil cleachdadh IDan-buidhne ceadaichte ach a-mhàin nuair a tha iad freagarrach airson na h-obrach a thathar a' dèanamh.

Each user within Bòrd na Gàidhlig is given a unique user ID to enable access to operating systems used for the generation, distribution, and storage of information. This unique ID ensures that users can be linked to and made responsible for their actions when accessing information. The use of group IDs is only permitted where they are suitable for the work carried out.

Feumar ath-sgrùdadh a dhèanamh air ceadan-inntrigidh àbhaisteach gu cunbhalach gus dèanamh cinnteach gu bheil na còraichean iomchaidh aig daoine fhathast.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated.

A'Di-chlàradh Chleachdaichean

User De-registration

Tha e an urra ri Manaidsearan-streatha Bòrd na Gàidhlig crìoch a chur air cunntasan aig luchd-obrach a tha gu bhith a' falbh tro bhith a' togail tiogaid le solaraiche nan seirbheisean ICT nuair a dh'fhàgas neach-obrach cosnadh Bhòrd na Gàidhlig. Feumaidh iad iarraidh gun tèid inntrigeadh air siostaman coimpiutair agus dàta a bhith

Bòrd na Gàidhlig line managers are responsible for employee termination control by raising a ticket with ICT managed service provider when an employee leaves Bòrd na Gàidhlig employment. Requesting access to computer systems and data be revoked and account suspended at the end of the employee's last working day.

air a thoirt air falbh agus an cunntas a bhith air a chur à comas aig deireadh an latha-obrach mu dheireadh aig an neach-obrach.

Tha Manaidsear Gnìomhan Bhòrd na Gàidhlig an urra ri bhith a' cumail smachd air dùnadh chunntasan airson buill a' bhùird-stiùiridh agus airson manaidsearan le bhith a' togail tiocaid leis an solaraidhe nan seirbheisean ICT. Feumaidh iad iarraidh gun tèid inntrigeadh air siostaman coimpiutair agus dàta a bhith air a thoirt air falbh agus a bhith air a chur à comas aig deireadh an latha-obrach mu dheireadh aig ball a' bhùird-stiùiridh no aig an àrd-mhanaidsear

Tha e an urra ri manaidsearan-streatha Bòrd na Gàidhlig no Manaidsear Gnìomhan tiogaid eile a thogail gus an cunntas a chaidh a chur à comas a sguabadh às taobh a-staigh sia mìosan bhon latha obrach mu dheireadh

A' Stiùradh Phrìobhaidean

Feumaidh cruthachadh cunntasan inntrigidh do chleachdaichean le prìobhaidean sònraichte leithid rianadairean a bhith fo smachd teann agus air an cuingealachadh ris an fheadhainn le uallach airson riaghladh no cumail suas an t-siostam fiosrachaidh no an lìonra a-mhàin. Tha an ìre inntrigidh seo aig solaraidhe nan seirbheisean ICT againn. Feumaidh cunntas rianachd sònraichte a bhith aig gach rianadair, nach eil air a chleachdadh ach airson adhbharan rianachd siostaim a-mhàin, agus a tha air a chumail air leth bhon chunntas inntrigidh àbhaisteach aig a' chleachdaiche.

Thèid cunntasan cleachdaiche ùr a chruthachadh agus a dhearbhadh tro iarrrasan airson atharrachaidhean, agus bu chòir tiocaid a thogail le solaraidhe nan seirbheisean ICT againn leis a' mhanaidsear loidhne aig Bòrd na Gàidhlig a tha an urra ris an neach-obrach. Thèid cunntas cleachdaiche a chruthachadh gus cothrom fhaighinn air na siostaman pròiseasaidh

Bòrd na Gàidhlig Operations Manager is responsible for board member and management termination control by raising a ticket with ICT managed service provider. Requesting access to computer systems and data be revoked and suspended at the end of the board member or senior managers last working day.

Bòrd na Gàidhlig line managers or the Operations Manager are responsible for raising a further ticket to have the disabled account deleted no longer than six months after the last working day.

Privilege Management

The creation of user access accounts with special privileges such as administrators must be rigorously controlled and restricted to only those who are responsible for the management or maintenance of the information system or network, our ICT managed service provider has this level of access. Each administrator must have a specific admin level account, which is only used for system administrative purposes, and is kept separate from their standard user access account.

New user accounts are created and validated through change request control, a ticket should be raised with our ICT managed service provider by Bòrd na Gàidhlig line manager responsible for the employee. The user account will be created to access the information processing systems with privileges restricted and controlled in accordance with job function.

fiosrachaidh, le prìobhaidean air an cuingealachadh agus air an stiùireadh a rèir dleastanasan obrach.

Feumar còraichean fo phrìobhaidean a bhith air an ùghdarrachadh le Ceann an Ionmhas is Cùisean Chorporra aig Bòrd na Gàidhlig a tha an urra ri còraichean inntigidh fo prìobhaidean air feadh na buidhne aig a' cheann thall.

Privileged access must be authorised by Bòrd na Gàidhlig Head of Finance and Corporate Affairs, ultimately responsible for privileged access rights across the organisation.

A' Stiùireadh Faclan-Faire nan Cleachdaichean

Bu chòir structar faclan-faire Bhòrd na Gàidhlig a bhith a rèir nan riaghailtean agus dòighean-obrach ann am poileasaidh nam faclan-faire.

Bòrd na Gàidhlig password structure should follow the rules and procedures set out in the password policy.

Dleastanasan a' chleachdaichean

Tha grunn dleastanasan air cleachdaichean a thaobh smachd air inntigeadh:

User Responsibilities

Users have many responsibilities relating to access control, these include:

A' gèilleadh ri teirmichean a' phoileasaidh seo fad an t-siubhail.

Complying with the terms of this policy at all times.

A' gèilleadh ri agus a' dìon phrìobhaideachd agus dìomhaireachd nan siostaman fiosrachaidh agus nan lìonraidhean a bhios iad a' cleachdadh, agus am fiosrachadh a tha air a phròiseasadh leis na siostaman no na lìonraidhean sin.

Respecting and protecting the privacy and confidentiality of the information systems and network they access, and the information processed by those systems or networks.

A' dèanamh cinnteach nach cleachd iad ach cunntasan agus faclan-faire a chaidh a shònrachadh dhaibh

Ensuring they only use user access accounts and passwords which have been assigned to them.

A' dèanamh cinnteach gu bheil na faclan-faire uile a th' aca air an cumail dìomhair fad an t-siubhail agus nach eil iad air co-roinn le duine sam bith eile, a' gabhail a-steach co-obraichean no treas-phàrtaidhean (mar a tha air a chur an cèill ann am poileasaidh nam faclan-faire).

Ensuring all passwords assigned to them are kept confidential at all times and not shared with others including their co-workers or third parties (as stated within the password policy).

Ag aithris gach mì-chleachdadh is briseadh den poileasaidh seo dhan mhanaidsear-streatha aca no do Mhanaidsear Gnìomhan aig Bòrd na Gàidhlig

Reporting all misuse and breaches of this policy to their line manager or Bòrd na Gàidhlig Operations Manager

Smachd air inntreigeadh dhan Lionra

Tha comas aig ceanglaichean lionra, gu sònraichte ceanglaichean eadar-lìn agus gun uèir, cunnartan cudromach agus neo-aithnichte a thoirt a-steach do dh'àrainneachd ICT Bòrd na Gàidhlig. Bidh solaraiche nan seirbheisean ICT againn a' sgrùdadh na h-àrainneachd ICT againn gu cunbhalach gus dèanamh cinnteach nach deach lionra sam bith a chur an sàs gun chead bhon sgioba stiùiridh.

Ma thèid PC'an nach eil air an stiùireadh le Bòrd na Gàidhlig a cheangal ri lionraidhean Bhòrd na Gàidhlig, is urrainn dhaibh droch bhuaidh a thoirt air tèarainteachd an lionraidh. Chan fhaodar bacadh a chur air obrachadh àbhaisteach nan lionraidhean ann an dòigh sam bith.

Feumar cead fhaighinn, an dàrna cuid sgrìobhte no beòil, bho sholaraiche nan seirbheisean ICT againn mus tèid uidheamachd sam bith a cheangail ri lionraidhean Bhòrd na Gàidhlig.

Smachd air inntreigeadh dhan t-Siostam-obrachaidh

Tha siostaman-obrachaidh nam prìomh shiostaman anns am bi aplacaidean gnìomhachais ag obair agus a' toirt seachad nan seirbheisean a dh'fheumar gus an gnìomhachas a ruith. Bu chòir cùram sònraichte a ghabhail gus an ìre iomchaidh de smachdan a chruthachadh gus na siostaman-obrachaidh a dhìon bho inntreigeadh gun chead, atharrachadh no bho bhriseadh a-steach air.

Thathar a' cumail smachd air agus a' dìon siostaman-obrachaidh tro dhòighean-obrach tèarainte airson clàradh a-steach agus dearbhadh. Mar a chaidh a chur an cèill na bu thràithe, tha cunntas cleachdaiche air leth aig gach cleachdaiche aig siostaman-obrachaidh Bhòrd na Gàidhlig agus feumar dòigh thèarainte a chleachdadh gus an cleachdaiche aithneachadh mus faigh iad inntreigeadh

Network Access Control

Network connections, particularly Internet and wireless connections, have the ability to introduce significant and unidentified risks into Bòrd na Gàidhlig ICT environment. Our managed service provider routinely monitor the ICT environment to ensure that no new networks have been implemented without management approval.

The use of non Bòrd na Gàidhlig managed PC's connected to Bòrd na Gàidhlig networks can seriously compromise the security of the network. The normal operation of the networks must not be interfered with in any way.

Specific approval, either written or verbal, must be obtained from our managed service provider before connecting any equipment to Bòrd na Gàidhlig networks.

Operating System Access Control

Operating systems are the core systems in which business applications function and perform the services required to operate the business. Special care will be taken to develop the appropriate layer of controls to protect the operating systems from unauthorised access, modification, or interruption.

Operating systems are controlled and protected by secure log-on and authentication procedures. As previously mentioned, each user of Bòrd na Gàidhlig operating systems have their own unique user account, and a secure method should be used to validate the user's identity before allowing access to the system.

dhan t-siostam.

Airson adhbharan tèarainteachd, às dèidh ùine ro-shuidhichte, bu chòir do shiostaman-obrachaidh agus coimpiutairean glasadh gus casg a chur air inntreigeadh gun chead.

For security reasons, after a predetermined amount of time, operating systems and terminals should lock to prevent unauthorised access.

Smachd air inntreigeadh do dh'aplacaidean agus do dh'fhiosrachadh

Application and Information Access Control

Feumar cothrom air fiosrachadh a tha ann an siostaman gnìomhachais a bhith air a dhìon a rèir a' Phoileasaidh Smachd air Inntreigeadh agus a rèir riatanasan aig aplacaid gnìomhachais iomchaidh sam bith.

Access to information contained in business systems should be protected in accordance with the access control policy and any applicable business application requirements.

Bu chòir inntreigeadh air aplacaidean a bhith air a chuingealachadh leis na feartan tèarainteachd a tha mar phàirt den bhathar fa leth.

Access to applications should be restricted using the security features built into individual product

Feumaidh inntreigeadh do dh'aplacaidean agus do dh'fhiosrachadh a bhith:

Access to applications and information must:

Air a roinn ann an dreuchdan a tha air an comharrachadh gu soilleir
A' toirt na h-ìre iomchaidh de dh'inntreigeadh a tha a dhìth air cleastanasan obrach a' chleachdaiche sin

Be separated into clearly defined roles
Give the appropriate level of access required for the role of the user.

Do-dhèante a bhith air atharrachadh gun ùghdarras (leis na roghainnean rianachd air an toirt air falbh no a bhith falaichte bhon chleachdaiche).

Be unable to be overridden (with the admin settings removed or hidden from the user).

Saor bho atharrachadh le còraichean a fhuair mar dhìleab bhon t-siostam obrachaidh a dh'fhaodadh ìrean inntreigidh nas àirde a thoirt do dhaoine gun chead

Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.

6 Cur an Gnìomh

Enforcement

Tha am poileasaidh seo èigneachail agus le bhith ag inntreigeadh goireasan teicneòlas conaltraidh fiosrachaidh sam bith a tha fo shealbh no air mhàl le Bòrd na Gàidhlig, tha cleachdaichean ag aontachadh gun cùm iad ri cumhachan a' phoileasaidh seo.

This policy is mandatory and by accessing any information communications technology resources which are owned or leased by Bòrd na Gàidhlig, users are agreeing to abide by the terms of this policy.