CYNGOR SIR
YNYS MÔN
ISLE OF ANGLESEY
COUNTY COUNCIL

Isle of Anglesey County Council
Administrative Access Security Policy

Version 1.2 (October 2026)

About this policy

This policy is an extension of the IT Security Policy, taking into consideration the additional obligations on users with administrative level access to any of the authorities ICT systems, digital services, or applications, such as system administrators within individual services and DDaT staff, where the existing policy may not fully safeguard the council from the risks associated with such elevated access.

The policy is relevant to all council staff who have administrative access to any of the authority's business systems, including where services have assigned local administrators for corporate systems and service specific systems which includes administrator access, and all DDaT staff with elevated access.

The main purpose is to ensure system administrators and DDaT staff are aware of their responsibilities in ensuring the authority's business systems adhere to existing IT policies and procedures, and actions to be taken in order to rectify or mitigate any identified noncompliant factors.

Revision history

Version	Date	Summary of changes
1.0.1	15 December 2025	Minor amendment
1.2	15 October 2026	Reviewed and updated to clarify security requirements.

Date of next review

This policy will be amended regularly in response to changing circumstances as digital technologies develop and in response to operational and legislative requirements.

This document will be reviewed in October 2027.

This document will be reviewed by the Lead Security Engineer.

Contact details

Gwyndaf Dale

Lead Security Engineer

gwyndafdale@anglesey.gov.wales

We are happy to provide this policy in alternative formats on request. Please use the above contact details.

Mae'r ddogfen yma ar gael yn y Gymraeg This document is available in Welsh

Contents

1. Introduction 4
2. Purpose 4
3. Scope 5
4. Passwords and account security 5
5. User maintenance and monitoring 6
6. Third party remote access 7
7. Legacy systems 8
8. Systems maintenance 8
9. Systems implementation 10
10. Asset disposal 11
11. Internal IT admin access for DDaT staff 11
12. Policy compliance 12
13. Review and revision 13

Weblinks 14

1. Introduction

1.1. The council recognises the risks associated with the configuration of business systems and the possibility of misalignment between the authority's Information Technology (IT) Security Policy and the settings used in individual business systems.

1.2. In ensuring that the council meets its legal requirements under the UK General Data Protection Regulations (UKGDPR), securing council data, particularly that classified as OFFICIAL-SENSITIVE is of paramount importance.

1.3. Loss, disclosure or corruption of such information could have a significant effect on the efficient operation of the council. It is therefore essential for the continued operation of the council that the confidentiality, integrity and availability of all information recording systems are maintained at a level which satisfies legislation and meets the council's needs.

1.4. This policy has been developed taking note of industry best practice, and aims to mitigate the following risks:

- significant disruption to the council's ability to provide statutory services as a result of a successful cyber attack
- disclosure of information as a consequence of loss, theft or careless use of IT equipment and storage media
- harm or distress to individuals caused by the disclosure of information
- contamination and disruption of council networks or equipment through the introduction of malicious or unwanted computer programs
- potential legal action against the council or individuals as a result of information loss or misuse
- potential sanctions against the council or individuals imposed by the Information Commissioner's Office (ICO) as a result of the above
- reputational damage as a result of information loss or misuse

1.5. This policy makes reference to other council policies and breach of a linked policy will be treated as a breach of the IT Security Policy[i].

2. Purpose

2.1. This policy aims to ensure that system administrators and DDaT staff are aware of their responsibilities in ensuring the authority's business systems

adhere to existing IT policies and procedures, and actions to be taken in order to rectify or mitigate any identified noncompliant factors.

3. Scope

3.1. This policy applies to all officers who hold administrative level access to any of the authorities Information and Communication Technology (ICT) systems.

4. Passwords and account security

4.1. Staff will never share their administrative login details or passwords with any other person.

4.2. Single sign on (SSO) is the preferred authentication method of the council and must be used, where available. If SSO is not available for administrative accounts as a minimum, the system must be reprocured at the earliest opportunity.

4.3. Where possible, multi factor authentication (MFA) methods must also be used for administrator accounts.

4.4. Where the system administrator also has general use of the system, the username/account used for undertaking administrative tasks should not be the same as the username/account used for general systems use.

For example:

A member of staff has both administrator and user level access to a business system, the user will log in to the system for day to day activities using a standard account such as 'rhxid'. If required to perform administrative tasks the user will log out and log in to undertake system changes as 'rhxid-sysadmin'.

4.5. A standard user account must never have administrative access to a system. Due to the enhanced security measures for administrative accounts, applying administrative access to a standard user increases the security risk to the council.

4.6. Where SSO is not available, administrative passwords must meet or exceed the enhanced password policy defined below:

- **minimum character length**: 16
- **complexity**: required
- **expiration**: 365 days
- **password reuse**: 24 months
- **failed logons**: 5 attempts

- **lockout duration**: 120 minutes, or until unlocked by an administrator
- **password minimum age**: 1 day

4.7. The above is considered a minimum and it would be best practice to use a longer passphrase made up of several unrelated words, for example: Dogs-Litigation-Picnic-230721!

4.8. Service level systems must support SSO for standard users or enforce a standard user password policy that meets or exceeds the corporate standard defined in the IT Security Policy[i], where SSO is not available.

4.9. Systems that are unable to meet these requirements will require additional mitigating actions based on the risk associated with the system. Users must contact the Digital, Data and Technology (DDaT) team as a matter of urgency where this standard cannot be met to ensure a program of work is undertaken to mitigate the risk.

4.10. Where it is not possible to enforce password complexity within a system, mitigating actions may be required that may limit system functionality and/or introduce additional costs. In such circumstances, discussions will be held to agree suitable budgets, which may be shouldered by the service. While a suitable alternative or development work is undertaken it is the responsibility of the system administrator to instruct staff that passwords must be manually set to meet these requirements. This requirement applies to all systems, regardless of the fact that the workstation is already protected by a password.

4.11. Services should ensure processes are in place and agreed with regards to who may be granted temporary administrative access in the absence of the system administrator, and only where required to ensure continuity of service.

5. User maintenance and monitoring

5.1. To prevent unauthorised persons from gaining access to sensitive elements of business systems the system administrators should employ the principle of 'least privilege'. The principle of 'least privilege' states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.

5.2. System administrators should ensure Role Based Access Control (RBAC) provisions are in place, including a comprehensive set of documentation outlining the process of creating/assigning users and the relevant system roles which should be applied to users based on their required access.

5.3. The systems administrators must provide details to the DDaT division of the users who have privileges which bring them within scope of this policy, the DDaT division will retain this information for audit purposes and policy compliance. The types of roles may include (but are not limited to):

- users who can make configuration changes to the system
- users who can assign, remove or modify user permissions
- users who can create, delete or change user accounts
- users who can view, create or delete Application Programme Interface (API) or system access tokens

5.4. When a system administrator receives a request to reset a user's password in a nonSSO application, a security check process should be used to ensure the request has come from an authorised user.

5.5. The system administrator must disable the accounts of leavers as soon as their end date is reached. Where possible, systems should be configured to use SSO to facilitate this, or where SSO is not possible, the service must ensure they request timely information on leavers.

5.6. The business system administrator should regularly review user activity and disable users who have not used the system within a 60 day period. In the event of long term staff absence, such as maternity leave, the account should be disabled at the start of the absence.

5.7. When provisioning/deprovisioning users, the system administrator must retain a record of starters and leavers for audit purposes, including their access level.

5.8. Information asset administrators are responsible for checking system records for anomalous or fraudulent activity. How regularly this should be carried out should be determined by the information asset owner's own risk assessments. Further guidance on the responsibilities of information asset administrators and information asset owners can be found on the information governance pages of Monitor[ii] or by contacting the Data Protection Officer (DPO).

6. Third party remote access

6.1. Where third party IT suppliers are granted remote access for support, the following controls must be applied to protect data and meet council security standards:

- third parties will only be provided with remote Virtual Private Network (VPN) login upon completion of a Remote Access Agreement form which records their agreement to abide by council IT policies as well as their commitment to a Data Processing Agreement

- access from external sources is not permitted via peer to peer remote access systems such as Microsoft Teams, Zoom, TeamViewer, GoToMeeting, and so forth - these methods have

been associated with well publicised cyber attacks and pose a potential risk to the security of the council's network

- VPN access will only be granted upon request to the IT Service Desk and will be revoked at the end of the working day - where urgent remote access is required the request should be made via telephone, not email

- no external third party (external contractors, partners, agents, the public or nonemployee parties) may extract information from the council's IT equipment without explicit agreement from the Chief Digital Officer or their delegated officers - a service based contact must ensure they have the authority to approve before actioning this, users can seek guidance from the DPO

7. Legacy systems

7.1. The council is part of the Public Sector Network (PSN). Being connected to the PSN allows the council to securely exchange sensitive data with the Department for Work and Pensions (DWP) and other local authorities. A condition of the council's connection to PSN is that it will ensure its IT systems meet a stringent set of security standards known as the Code of Connection, which includes undertaking an annual IT Health Check (ITHC).

7.2. As well as being accepted good practice, the PSN require that the council only uses software and hardware which is still maintained by the vendor so that if any security vulnerabilities are discovered in that technology, they may be updated as required. Systems which are no longer maintained by their vendor are, for the purposes of this document, described as 'legacy systems'.

7.3. Using legacy software is considered by the Cabinet Office to be a security risk not only to the council, but to other organisations connected to the PSN and as such would result in failure of the annual PSN assessment.

7.4. It is for this reason that all legacy systems will be removed from the network once the vendor has withdrawn support. Where the data held in the legacy system must be retained, then it should be exported to a supported format, for example a newer version of the software.

7.5. It is the responsibility of the administrator of legacy systems to develop a plan to migrate the data within the system to another suitable format or system to allow the legacy one to be decommissioned. Where this is not undertaken, the system will be disabled.

8. Systems maintenance

8.1. To protect the confidentiality, integrity and availability of the council's data and systems, service administrators must ensure plans are in place to keep ICT systems, for which they are responsible for, up to date and free from vulnerabilities.

8.2. Where a system relies on scheduled jobs/tasks, they should all be set up with a system specific generic service account which is not used by system administrators for any other reason. This protects the system against failure where an account is deprovisioned/disabled. For example, if Admin A has set up scheduled jobs to run reports, and then their account is disabled due to leaving, the reporting job would no longer run. Configuring jobs with a service account means they are not reliant on a user's account being enabled.

8.3. Service administrators will ensure system updates or 'patches' are scheduled appropriately and in line with update periods noted below. Administrators are responsible for ensuring testing is undertaken and to communicate changes or any downtime to system users. Administrators must ensure they have a means of receiving notifications of application updates and patches or proactively enquire with the vendor or utilising any provided knowledge sites for the relevant systems.

8.4. Service administrators must inform their relevant DDaT contact of any planned updates and/or scheduled maintenance in order to ensure impact on any other users or processes can be minimised accordingly. Where such updates or maintenance require direct input from the DDaT team, sufficient notice must be provided to ensure adequate resources and expertise are available accordingly.

8.5. The DDaT division will inform service administrators of vulnerabilities identified in applications they manage. Service administrators will assist the DDaT division with remediation and are required to action these in accordance with the timelines set out by the DDaT division. The timeline will be set according to an assessment of risk.

8.6. System administrators must ensure that any exploitable vulnerability is managed, known as vulnerability or patch management. System administrators must have a defined policy and supporting process to identify, prioritise and mitigate all vulnerabilities. Policies will outline specific updates or patch application periods and a process for auditing compliance.

8.7. The below values are the maximum threshold, and the assessment undertaken by the DDaT division may require updates to be applied sooner.

System type	Critical severity	Severe severity	Moderate severity
Public/internet facing	less than 2 days	less than 3 days	less than 5 days
Internal system/server	less than 3 days	less than 7 days	less than 14 days
User and client devices	less than 3 days	less than 7 days	less than 14 days

8.8. Where system administrators know that a vulnerability is being actively exploited, then updates should be actioned immediately where possible, or any other suitable mitigating actions in the interim.

8.9. Where an update is not deployed (or available) within the timescales above then there must be alternative mitigating action, such as disabling or reducing access to the vulnerable service.

8.10. It is important that issues identified in the annual ITHC are addressed. Critical and high risks should be addressed through upgrade or removal of an unsupported system, while medium and low risks may be accepted or subject to remedial action plans. Failure to address identified issues may affect the council's PSN accreditation and adversely impact our ability to deliver key services to residents.

8.11. The inability of a system administrator to test and deploy an update may not be used as a reason to defer applying an update. Where a system administrator is unable to do so they must contact the DDaT division in order for a plan to mitigate the risk to be developed. The mitigations may limit system function and/or introduce a financial burden. In such circumstances, discussions will be held to agree suitable budgets, which may be shouldered by the service..

8.12. Applications which no longer receive updates present a security threat to the council and service administrators must ensure plans are in place to retire systems that are no longer maintained ensuring any data is extracted and maintained in a secure and accessible format in accordance with the service's retention schedules. See Legacy systems section for further information.

9. Systems implementation

9.1. For the purposes of this policy, the re-procurement, contract renewal, material upgrade, migration, or replacement of an existing system shall be treated as a new procurement activity and must be assessed against the current security requirements and IT Technical Specification.

9.2. Any systems identified that have not been procured in partnership with the DDaT division will not be implemented and actions will be undertaken to prohibit access to and use of the application.

9.3. The following security standards will be considered a minimum requirement when procuring new IT systems:

- the system should be configurable to use SSO, failing this, the system must meet the password standards defined above

9.4. For new systems which are hosted external to the council (in the 'cloud'), the supplier will be required to complete a Data Processing Agreement which commits them to meeting the required security standards of the council, including (but not limited to):

- holding the data within the UK
- enforcing password complexity
- carrying out regular testing of security using accredited and independent third parties

9.5. A full set of requirements is outlined in the IT Technical Specification included within the procurement handbook, noncompliance with critical criteria will constitute a failure and the system will not be implemented.

9.6. Where an application is unable to comply with the email security requirements of the IT Security Policy[i], its ability to send emails via or on behalf of the authority will be removed.

10. Asset disposal

10.1. All equipment related to the business system which is no longer required shall be returned to the DDaT Division in line with the IT Asset Disposal Policy[iii], and by completing a 'Redundant IT Collection Form[iv], on the IT Service Desk Portal.

11. Internal IT admin access for DDaT staff

11.1. DDaT staff currently adhere to separation of admin and standard accounts. Occasionally, a DDaT staff member may require elevated access for particular tasks. Due to the nature of admin access to elements of Microsoft Azure and other Microsoft cloud platforms, elevated permissions introduce an inherent risk to the Microsoft tenant and must be considered under strong scrutiny and approval.

11.2. Where elevated access is required, the DDaT staff member must first open a Fresh Service ticket using the Request Admin Access[v] service request.

11.3. Full details must be included, and the ticket must be complete. Details will include the specific Microsoft role required, the purpose of the request and a specific timeframe where permissions are required. Timeframes should be considered carefully as role assignment will not be extended and once expired, a new request must be submitted. Once the ticket has been opened, it will be assigned to the staff member's line manager, and the request must be approved before it will be actioned by the Infrastructure Team.

11.4. The line manager must consider the requester's job description and whether it aligns with the purpose of the request and the permissions they are requesting. There is an element of responsibility on the line manager for the staff member's actions within the Microsoft tenant, and this must be considered carefully.

11.5. Once permissions have been assigned the admin account may be placed on a 'watchlist' where additional scrutiny will be applied to the actions performed by that account. The Infrastructure Team reserves the right to revoke access immediately if newly assigned permissions are used outside the stated scope of work. If a role/permissions are revoked under these circumstances, new requests by that staff member may be denied on this basis.

12. Policy compliance

12.1. Noncompliance with this policy could have a significant effect on the efficient operation of the council, result in a breach of the law and result in monetary penalties being levied on the council – accordingly, noncompliance should be dealt with by line managers via the appropriate competency and disciplinary procedures.

12.2. Where the DDaT division are made aware of, or encounter evidence of a breach of this policy a summary of the findings will be provided to an appropriate body or senior officer.

12.3. The DDaT division may include recommendations such as:

- an individual (or team's) IT policy acceptance and elearning status to be reset
- administrative access to relevant ICT systems to be revoked pending the outcome of an investigation
- administrative access to relevant ICT systems removed permanently

12.4. In the event of repeated breaches, the DDaT division's only recommendation will be the removal of administrative access to relevant ICT systems.

12.5. If any user is found to have breached this policy, they may be subject to disciplinary action. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

12.6. The DDaT division will request evidence of compliance with elements of this policy, service administrators must provide the requested evidence within the timelines of the exercise.

12.7. Failure to provide the evidence will be treated as a breach of this policy.

12.8. Where evidence indicates misconfiguration, the DDaT division will outline the action(s) required and provide reasonable time (in proportion to risk) for changes to be made and communicated.

12.9. Service administrators must rectify issues promptly, failure to do so will be treated as a breach of this policy.

12.10. If you do not understand the implications of this policy or how it may apply to you, seek advice from the DDaT Division.

13. Review and revision

13.1. This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

13.2. Policy review will be undertaken by the DDaT Division and authorised by the Senior Leadership Team.

Weblinks

[i] https://monitor.anglesey.gov.wales/policies/information-technology/IT-Security-Policy.pdf
[ii] https://monitor.anglesey.gov.wales/en-gb/council-functions/legal/information-governance
[iii] https://monitor.anglesey.gov.wales/policies/information-technology/it-asset-disposal-policy.pdf
[iv] https://desggymorth.ynysmon.gov.uk/support/solutions/articles/50000069360-how-do-i-dispose-of-redundant-it-equipment-
[v] https://desggymorth.ynysmon.gov.uk/support/catalog/items/317