Part of Objective B - Protecting against cyber attacks and data breaches

# Principle: B2 Identity and access control

← Previous Chapter

Principle: B1 Policies, processes and procedures

Current Chapter

Current chapter – Principle: B2 Identity and access control

View all

Next Chapter →

Principle: B3 Data security

## Page contents

# B2.a Identity verification, authentication and authorisation

> "You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s)."

## Overview

This outcome relates to your organisation having cyber security and information governance (IG) controls in place to ensure staff have appropriate access to information.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

## Initial identity verification

**(This is an increase in requirements for 2024-25 'Standards met')**

You should conduct pre-employment checks to appropriately identify individuals before allowing access to information, systems and networks. This should include contacting and verifying referees.

When establishing a person's identity, you should consider:

- the baseline checks you need to perform before allowing people to access your systems – health and care organisations undertaking the Cyber Assessment Framework (CAF)-aligned DSPT should already be vetting all staff members to NHS Employment Check or Baseline Personnel Security Standards
- the level of access they will have to your systems - the more sensitive or privileged their access, the stronger the identity verification you should perform
- whether certain roles should require more stringent background checks or security clearances - the more sensitive or privileged their access, the stronger the case for performing higher levels of identity verification

See NCSC guidance on identity and access management for more information.

## Individually identifying and authenticating

All instances of access to personal confidential data on IT systems should be attributable to specific individuals.

Staff members should access information, systems and networks using their own individual credentials. You should understand the roles and associated individuals with authorisation to access each information asset, system or network.

To preserve the one-to-one relationship between users and accounts, staff members should be aware that they hold responsibility for ensuring they:

- never share their password with anyone else
- never allow anyone else to use their smartcard
- never leave their smartcard unattended
- always remove their smartcard from the reader when they have finished using it

These obligations are not only essential measures for data security, but also form part of the terms and conditions of access to NHS Spine applications.

There may be some scenarios where there is a clear operational justification for using shared credentials. For example, in emergency planning, you may decide that it is appropriate for your organisation to keep laptops with generic user accounts for emergency use. In this scenario, you would apply additional security measures to keep the credentials secure and carefully manage access to them.

## Temporary staff members

Where staff members are provided by an external temporary staffing agency, your organisation should have gained sufficient confidence that the agency's identity check and validation procedures are as robust as your own.

For temporary staff members called at short notice, there could be scenarios where it would be impractical to undergo the verification, authentication and authorisation activities prior to account provision, which you undertake for your permanent or longer-term temporary members of staff.

In these scenarios, you should take a risk-based approach to granting access to systems. You should have appropriate technical and procedural controls in place to ensure that all activities can be traced back to specific individuals, and that where accounts are temporarily assigned, they can only be accessed by a single person within a determined time frame.

Centrally managed credentials such as NHSmail identities should be considered to provide additional authentication for temporary staff members accessing your systems.

## Limiting authorised users and systems

You should ensure that staff members are granted access to information proportionally, so that they have exactly the level of access they need to fulfil their roles.

Role-based access controls are key to achieving these requirements, and ‘least privilege’ should be a guiding principle. If a user only needs to view records, for example, there is no need for them to have an elevated role such as ‘admin’ or ‘super user’. The ‘view-only user’ role will give them the level of access they require.

Your procedures should also ensure that access is removed from users as soon as it is no longer required. For this, your access controls need to be appropriately joined up with your processes for joiners, movers and leavers.

For each information asset, system or network supporting your essential functions, you should know the way that identity and access management procedures have been applied to achieve the desired outcome.

## Additional authentication mechanisms

It is a requirement of the NHS England multi-factor authentication (MFA) policy that MFA is used on digital systems throughout the health sector, with particular requirements on accounts that are remotely accessible or have privileged access to systems.

See guidance on the NHS England multi-factor authentication policy for more information.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents (for example, identity verification, identity and access management, joiners/movers/leavers)
- mitigations in place for systems that do not use individual logins
- records of authorised user accounts and level of access
- network accounts audits
- logs of security incidents and follow-up actions

This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

| | |
|---|---|
| **Indicator(s) of good practice** | PA#1<br>Your process of initial identity verification is robust enough to provide a reasonable level of confidence of a user’s identity profile before allowing an authorised user access to information, systems and networks that support your essential function(s). |

| | |
|---|---|
| Term | 'essential function(s)' |
| Interpretation | Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions.<br>For more information, see guidance on scoping essential functions. |

| | |
|---|---|
| Indicator(s) of good practice | PA#7<br>A#6<br>Your approach to authenticating users, devices and systems follows up to date best practice. |
| Term | 'up to date best practice' |
| Interpretation | Following up to date best practice means that you should be able to justify the technical and physical access management controls you have in place, and consider practical improvements based on the emergence of new technologies and knowledge sharing with other professionals in your network. |

## Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control
National Cyber Security Centre | Introduction to identity and access management
NHS England | Cyber assurance service
NHS England | Technical remediation service
Information Commissioner's Office | Records management and security – access control

## Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

# B2.b Device management

> “You fully know and have trust in the devices that are used to access your information, systems and networks that support your essential function(s).”

For this contributing outcome, there is no minimum expected level of achievement for 'Standards met'. You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation's cyber security and information governance (IG) activities. The Data Security and Protection Toolkit (DSPT) 'Standards met' expectation should be regarded as a minimum compliance level, not the end goal of your organisation's cyber security and IG activities.

## Overview

To achieve this outcome you need to understand the scope and security characteristics of devices connected to your network.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 DSPT framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

## Corporately owned and managed devices

Your corporately owned and managed devices should be securely configured, making it possible for staff members to perform their roles while mitigating the risk of system compromise by attackers. See NCSC guidance on device security for more information.

You should ensure that the number of privately owned devices such as bring your own devices (BYOD) is kept to the minimum amount necessary to sustain your essential function(s). You should also ensure you have managed data protection risks for the use of any privately owned devices connected to your network.

## Third-party devices

You should have a process in place to minimise the risks presented by third party devices connected to your network, including privately owned devices (Bring Your Own Devices). This may include:

- conducting checks (such as scanning for malware)
- restricting devices that can connect to your network, such as through network access control
- having contractual data protection and security obligations in place with third-party device providers
- segmenting your network to isolate third-party devices

You should be aware of the risks and be assured that adequate mitigations are in place before allowing third-party devices to connect to your network.

## Privileged access

Privileged operations such as system administration should only be carried out from corporately owned and managed devices, with controls in place to separate those privileged operations from normal user activity. Examples of this type of control include:

- issuing users with separate privileged accounts that have no access to the internet, email, or other higher-risk resources used by normal user accounts
- 'browse-up' administration, such as using an ordinary device to access a remote desktop environment for privileged operations - this approach is not recommended (see NCSC guidance on the 'browse-up' anti-pattern) but you may decide the risk is tolerable for a period of time while you implement a better solution
- 'browse-down' administration, such as using a highly-trusted device to access a remote desktop environment for normal user activities - this can include thin clients accessing multiple remote environments separated for privileged and normal user activities
- dedicated Privileged Access Workstations, specifically configured and protected for privileged operations and not used for any other activity

Wherever possible, the administration of a system should be performed from a device that is trusted to at least the same level as that system.

If you have third party suppliers carrying out privileged operations, you should seek assurance (or set requirements) on the devices and architectures used – see NCSC guidance on systems administration architectures for examples and further information.

Although the expected interpretation of 'privileged operations' is narrow and relates only to security-relevant functions, you are likely to have other users with access to perform business-critical functions or to effect wide-ranging changes (such as finance users approving large payments, or software developers committing changes to code repositories). You should consider whether it is appropriate to apply the same or similar controls to those users and devices, based on risk.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents relating to network security and corporate devices
- assessment and evaluation protocols for third-party devices / systems
- asset discovery scans

This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

| | |
|---|---|
| **Indicator(s) of good practice** | PA#1<br>Only corporately owned and managed devices can access your essential function(s)'s networks and information systems. |
| **Term** | 'corporately owned and managed devices' |
| **Interpretation** | These devices may belong to your organisation, or they might be provided by a third-party supplier. They should be fully governed by your corporate IT policies.<br>Privately owned devices for example bring your own devices (BYOD) do not fall in this category. |

| | |
|---|---|
| **Indicator(s) of good practice** | PA#1<br>Only corporately owned and managed devices can access your essential function(s)'s networks and information systems. |
| **Term** | 'essential function(s)' |
| **Interpretation** | Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions.<br>For more information, see guidance on scoping essential functions. |

| | |
|---|---|
| **Indicator(s) of good practice** | PA#2<br>All privileged operations are performed from corporately owned and managed devices. These devices provide sufficient separation, using a risk-based approach, from the activities of standard users.<br>A#1<br>All privileged operations performed on your network and information systems supporting your essential function(s) are conducted from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations. |
| **Term** | 'privileged operations' |

| | |
|---|---|
| **Interpretation** | Privileged operations are actions that could have a significant impact on the system. |

## Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control
National Cyber Security Centre | Introduction to identity and access management
National Cyber Security Centre | Security architecture
National Cyber Security Centre | Device security guidance
NHS England | Network segmentation architecture patterns for connected medical devices
NHS England | Cyber assurance service
NHS England | Bring your own device (BYOD) guidance
Information Commissioner's Office | Bring your own device (BYOD)

## Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

# B2.c Privileged user management

> "You closely manage privileged user access to networks and information systems supporting your essential function(s)."

For this contributing outcome, there is no minimum expected level of achievement for 'Standards met'. You are still required to assess your achievement level and provide a response, showing you have considered the implications of the contributing outcome for your organisation's cyber security and information governance (IG) activities. The Data Security and Protection Toolkit (DSPT) 'Standards met' expectation should be regarded as a minimum compliance level, not the end goal of your organisation's cyber security and IG activities.

## Overview

This outcome relates to you ensuring that privileged users are authenticated, monitored and managed effectively.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 DSPT framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

## Authentication

It is a requirement of the NHS England multi-factor authentication (MFA) policy that MFA is used on digital systems throughout the health sector, with particular requirements on accounts that are remotely accessible or have privileged access to systems.

See guidance on the NHS England multi-factor authentication policy for more information.

## Privileged access

You should know who has privileged access to systems within your organisation. Due to these accounts having an elevated level of privileged access, it becomes more important to revoke access when they no longer need it.

Reviews of privileged user access should not only be triggered when individuals leave the organisation, but also when their role changes within the organisation.

## Reviewing and validating privileged user activity

You should log privileged user actions so that they can be independently reviewed and audited.

To monitor privileged user activity most effectively, you should also define rules that detect suspicious activity and trigger active reviews of events. These rules could highlight when certain commands are run by administrators, or when changes are made at odd times, or in an unusual quantity. You should consider specific review practices for privilege operations carried out by external contractors and third parties such as suppliers.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- register of privileged accounts
- policy, process, procedure or strategy documents relating to privileged user access management
- privileged user signed agreements
- logs of privileged user activities
- dormant accounts reports

This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

| | |
|---|---|
| **Indicator(s) of good practice** | PA#1<br>All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor authentication (MFA). |
| **Term** | 'privileged user(s)' |
| **Interpretation** | A user that is authorised (and therefore, trusted) to perform privileged operations that standard users are not authorised to perform. Privileged operations are actions that could have a significant impact on the system. |

| | |
|---|---|
| **Indicator(s) of good practice** | PA#1<br>All privileged user access to network and information systems supporting your essential function(s) requires strong authentication, such as multi-factor (MFA). |
| **Term** | 'essential function(s)' |
| **Interpretation** | Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions.<br>For more information, see guidance on scoping essential functions. |

## Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control

National Cyber Security Centre | Introduction to identity and access management

NHS England | Cyber assurance service

NHS England | Technical remediation service

## Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

# B2.d Identity and access management (IAM)

> “You closely manage and maintain identity and access control for users, devices and systems accessing the network and information systems supporting your essential function(s).”

## Overview

To achieve this outcome, your organisation needs to demonstrate that you closely manage and maintain identity and access controls for your information, systems and networks.

## Mapping to the 23-24 DSPT framework

Under the previous 23-24 Data Security and Protection Toolkit (DSPT) framework, your organisation was required to perform activities that help meet the expectations of this contributing outcome.

For more detail on what these activities were, see the mapping exercise published by NHS England and Department of Health and Social Care (DHSC).

**(This is an increase in requirements for 2024-25 ‘Standards met’)**

### Verifying users

Please see ‘B2.a Identity verification, authentication and authorisation’ for information about verifying users.

### Issuing minimum access rights

You should ensure that staff members can only access the information and systems that are necessary to allow them to perform their role. This means that there should be no 'one-size-fits-all' permissions configuration for all staff members.

You should configure all your devices to issue permissions to staff members based on the principal of ‘least privilege’, and segment users by their role. If a user only needs to view records, for example, there is no need for them to have an elevated role such as ‘admin’ or ‘super user’. The ‘view-only user’ role will give them the level of access they require.

For each information asset, system or network supporting your essential function(s), you should know the way that identity and access management procedures have been applied to achieve the desired outcome.

## Logging and monitoring user, device and system access

You should have logs showing when users have accessed your systems, and a process for reviewing the logs at appropriate intervals.

To obtain the best active view of users, devices and systems accessing systems supporting your essential function(s), the monitoring process can be automated from a central security information and event management (SIEM) tool. However, you will still need to have manual reviews of access logs in place for systems that cannot be integrated into a SIEM tool.

## Access issues

The people who know best what information and systems they need to access to perform their role are your staff members. Staff should understand their responsibilities, including their obligation to access and use information responsibly, in line with the Caldicott Principles.

Your organisation should have channels of communication for staff members to report when access protocols are not working. For example, members of the clinical team being unable to view patient records they need to provide care. You should be open to revising access procedures and permissions without undue delay in situations where staff are experiencing access issues, carrying out appropriate checks to ensure their suggestion is legitimate and granting more access is necessary.

## Supporting evidence

To support your response, you can review and upload (or link to) evidence which best demonstrates your achievement of the contributing outcome. Examples include:

- policy, process, procedure or strategy documents relating to identity verification, identity and access management, joiners/movers/leavers
- records of authorised user accounts and level of access
- access logs
- network accounts audits
- logs of security incidents and follow-up actions

This is not an exhaustive list. You're welcome to provide other types of evidence if you feel they are relevant to the contributing outcome.

Your supporting statement should cross-reference how each piece of evidence provides justification for your achievement of the contributing outcome, including relevant page numbers where appropriate.

## Interpreting indicators of good practice

| | |
|---|---|
| **Indicator(s) of good practice** | PA#2<br>You regularly review access rights and those no longer needed are revoked. |
| **Term** | 'regularly' |
| **Interpretation** | On a scheduled basis, with enough frequency to mitigate the risks associated with rights not being revoked in a timely fashion. |

| | |
|---|---|
| **Indicator(s) of good practice** | PA#4<br>All user, device and system access to the systems supporting the essential function(s) is logged and monitored, but it is not compared to other log data or access records. |
| **Term** | 'essential function(s)' |
| **Interpretation** | Your essential functions should be identified in a scoping exercise which you carry out before beginning your DSPT submission. The same exercise should identify all the information, systems and networks which support your essential functions.<br>For more information, see guidance on scoping essential functions. |

## Additional guidance

For additional guidance, see:

National Cyber Security Centre CAF guidance | B2 Identity and access control

National Cyber Security Centre | Introduction to identity and access management

NHS England | Cyber assurance service

NHS England | Microsoft Defender for Endpoint service

Information Commissioner's Office | Records management and security – access control

## Mapping to other cyber frameworks

NHS England and DHSC have produced a mapping document showing where the requirements of the CAF-aligned DSPT overlap with those of other cyber frameworks. New frameworks will be added to this document over the course of the year.

Last edited: 19 September 2024 2:37 pm

← Previous Chapter

Principle: B1 Policies, processes and procedures

Next Chapter →

Principle: B3 Data security

## Chapters

Facebook

LinkedIn

YouTube