National Cyber Security Centre

# GUIDANCE

The NCSC is part of the Government Communications Security Bureau

**05 November 2019**

# Improving Information Security: The Importance of Policies and Procedures

*On 9 May 2019, the Office of the Auditor General distributed a letter to all chief executives and board chairs, of central government organisations outlining reflections and insights from the 2017/18 central government audit work.*

*Weak information security (Infosec) policies and procedures, and inappropriate user access to networks and systems, were identified as key risks for many government agencies. The National Cyber Security Centre (NCSC) has developed the following guidance to help agencies address these issues and improve their Infosec capability and maturity.*

## Recommendations

- Implement timely security patching of operating systems, applications, and devices.
- Restrict privileged user access to limit your exposure to Infosec risk.
- Implement and enforce strong password policies.
- Undertake periodic formal reviews of user accesses to keep security measures up-to-date.
- Disabling ex-staff members access to agency systems.
- Implement strong change management processes for information systems.
- Review Infosec policies to ensure they reflect changes in your technology environment.

# Security Patching

## Implement timely security patches and other security measures

Over the course of a normal product lifecycle, patches are released to address known security vulnerabilities. Applying patches to operating systems, applications and devices is critical to ensuring the security of your agency's systems.

You are required to undertake patching and other security measures in accordance with the New Zealand Information Security Manual (NZISM) and the Protective Security Requirements (PSR) framework. This includes:

- applying all critical security patches as soon as possible and within two days of the release of the patch or update[i]
- implementing a patch management strategy, including an evaluation or testing process[ii]
- applying all non-critical security patches as soon as possible[iii]
- ensuring that security patches are applied through a vendor recommended patch or upgrade process.[iv]

### Monitoring

It is important that you monitor relevant sources for information about new vulnerabilities and security patches. This way, your IT department can take proactive steps to address vulnerabilities across the network by applying necessary security patches.

### Risks

Products and systems that are not patched create an opportunity for hostile actors to attack your network. This makes your agency a desirable target for cyber-attack, which may result in unauthorised access to official information, data compromise or loss and potential systems shutdown.

**Remember!**

It is essential that security vulnerabilities are patched as quickly as possible. Once vulnerabilities in an operating system, application or device are made public, it can be expected that adversaries will develop malicious code (also known as malware) within 48 hours.[v]

Additional advice about patching and security measures for information systems can be found on the Australian Cyber Security Centre website using the links below:

- the Essential Eight
- Strategies to Mitigate Cyber Security Incidents
- Assessing Security Vulnerabilities and Applying Patches

For more information about the information security standards you must meet, please refer to the following measures:

| | |
|---|---|
| **Protective Security Requirements**<br>• INFOSEC4 (analyse evolving threats and vulnerabilities, keep your information security measures up to date, respond to information security incidents) | https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |
| **NZISM Chapter 6 (Information Security Monitoring)**<br>• NZISM 6.2 (vulnerability analysis)<br>• NZISM 6.3 (change management) | https://www.nzism.gcsb.govt.nz/ism-document#738 |
| **NZISM Chapter 12 (Product Security)**<br>• NZISM 12.4 (product patching)<br>• NZISM 12.5 (product maintenance and repairs) | https://www.nzism.gcsb.govt.nz/ism-document#759 |

## Enforce strong password policies

### Password policies that are weak or not enforced create risks

Passwords are the main authentication tool agencies use for their staff to access computer systems. Therefore, it is essential that your agency has strong policies to guide how you develop and manage passwords across your network. It is a mandatory requirement under the PSR framework to develop and maintain security policies and plans that meet your organisation's specific business needs (GOV2), including password policies.

**Policy development**

The NZISM provides guidance for agencies to help them develop strong Infosec policies and SOPs. As part of your compliance with the NZISM, your internal Infosec policy should include information for choosing and protecting passwords (NZISM 5.5.6.C.01). Strong password policies must include standard operating procedures for:

- password selection
- password authentication
- password management.

Additional advice about password security can be found on the NZISM website here.

**Policy enforcement**
Robust policy can be rendered ineffective if it is not properly enforced. Compliance with password policies should be routinely monitored and tested in conjunction with regular education and training for employees about the importance of Infosec and maintaining password security.

**Risks**
Weak passwords and/or a relaxed security culture within your agency provide adversaries with a prime target for accessing your network. This can result in unauthorised access to sensitive or classified information, data compromise or an attack on your systems (such as a malware or ransomware attack).

Passwords are subject to three principal groups of risks, specifically intentional password sharing (insider threat), password compromise (theft or loss) and password guessing and cracking.

Poor password development (weak passwords) and poor password management practices expose your agency to increased levels of risk. This includes:

- passwords that do not comply with the recommendations in the NZISM
- passwords that are not changed regularly
- password management issues such as employees re-using the same passwords across different systems/accounts and storing passwords insecurely.

**Remember!**

Strong Infosec policies are easily undermined by weak security culture. Promoting a strong Infosec culture within your agency is essential to mitigating password security risks and can be enhanced with regular education, training and monitoring.

For more information about the information security standards you must meet, please refer to the following measures.

| | |
|---|---|
| **Protective Security Requirements**<br>• GOV2 (develop and maintain security policies and plans that meet your organisation's specific | https://protectivesecurity.govt.nz/governance/mandatory-requirements-2/ |

| | |
|---|---|
| business needs)<br>• INFOSEC2 (implement agreed security and privacy measures including polices, processes and technical security measures)<br>• INFOSEC3 (confirm that your information security measures have been correctly implemented and are fit for purpose)<br>• INFOSEC4 (maintaining appropriate access to your information) | https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |
| **NZISM Chapter 5 (Information Security Documentation)**<br>• NZISM 5.5.6 (system user SOPs) | https://www.nzism.gcsb.govt.nz/ism-document#676 |
| **NZISM Chapter 9 (Personnel Security)**<br>• NZISM 9.1.5 (degree and content of information security awareness and training) | https://www.nzism.gcsb.govt.nz/ism-document#1437 |
| **NZISM Chapter 16 (Access Control)**<br>• NZISM 16.1.23 (password selection policy)<br>• NZISM 16.1.24 (password management)<br>• NZISM 16.1.25 (resetting passwords)<br>• NZISM 16.1.26 (password authentication) | https://www.nzism.gcsb.govt.nz/ism-document#1801 |

## Restricting privileged access to those that need it

### Inappropriate access to information systems, including administrative access and "super user" accounts, exposes you to risk

Ensuring that people have access to the systems they need to do their job is essential for being able to deliver core business targets. However, inappropriate user access exposes your agency to a number of information security risks. Inappropriate user

access can occur when policies are weak, user access is not regularly reviewed or there is limited understanding about the Infosec risks associated with user access within your organisation. For example, your senior executives do not need administrator rights.

It is a mandatory requirement under the PSR framework to manage access rights, security passes and assets within your organisation (PERSEC3) and that you maintain appropriate access to your information (INFOSEC4). The NZISM outlines detailed requirements for access management and steps that must be taken to comply with Infosec standards.

**Making sure staff and contractors have appropriate user access**
It is essential to ensure that staff and contractors have access to information and systems that is in line with the specifications of their role. Only administrative users should have the ability to make changes to databases and systems.

**Risks**
Inappropriate user access can expose agencies to a number of risks, including staff gaining unauthorised access to restricted or sensitive information; staff implementing unauthorised changes to data or systems resulting in data corruption or loss; information being replicated or distributed outside of the network resulting in data loss and potential breach of privacy or security protocols.

**Remember!**

User access should be monitored regularly to ensure that information and systems are being used in line with agency policies.

User access should be reviewed when an employee changes their role within the organisation to make sure their user access remains appropriate.

User access for contractors, who may introduce additional risks, also requires security risk management - use the same personnel security measures with contractors as you would with permanent employees.

**Administrative access**
Users with administrative privileges for operating systems and applications are able to undertake a variety of actions including:

- making significant changes to the configuration and operation of the system or network
- bypassing critical security settings
- accessing sensitive information.

**Risks**
Adversaries often use malicious code (also known as malware) to exploit security vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.[vi]

**Remember!**

Only trusted personnel should be granted privileged access to systems.

Restricting administrative privileges is one of the most effective mitigation strategies in ensuring the ongoing security of systems.

Limiting the total number of privileged users means that fewer users can make significant changes to the operating environment, either intentionally or unintentionally.

Administrative or privileged systems access should be monitored and reviewed regularly to effectively manage any identified risks.

The Australian Cyber Security Centre (ACSC) website offers additional guidance about administrative access and privileged user access:

- https://www.cyber.gov.au/publications/restricting-administrative-privileges
- https://www.cyber.gov.au/publications/secure-administration

For more information about the information security standards you must meet, please refer to the following measures:

| | |
|---|---|
| **Protective Security Requirements**<br><br>• PERSEC3 (managing access rights, security passes and assets)<br><br>• INFOSEC4 (maintaining appropriate access to your information) | https://protectivesecurity.govt.nz/personnel-security/mandatory-requirements/<br><br>https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |
| **NZISM Chapter 16 (Access Control)**<br><br>• NZISM 16.1 Identification and Authentication<br>• NZISM 16.2 System Access<br>• NZISM 16.3 Privileged Access<br>• NZISM 16.4 Remote Access<br>• NZISM 16.5 Event Logging and Auditing | https://www.nzism.gcsb.govt.nz/ism-document/#1801 |

## User Access Policy: Implement reviews of user accesses

### Failure to perform or document formal reviews of user access creates risk

It is a mandatory requirement under the PSR framework to keep your security measures up to date by maintaining access control systems (INFOSEC4). PSR mandatory requirement GOV2 also requires that you must develop and maintain security policies and plans that meet your organisation's specific business needs.

An essential part of fulfilling both of these requirements is undertaking regular user access reviews and documenting this appropriately.

**Risks**

- Failure to regularly review and document your user access settings creates a significant weakness in your agency's information security posture. Failure to undertake regular auditing means that user access issues (such as inappropriate user access or data corruption) remains unidentified, preventing your agency's IT department from addressing these risks.

- Documenting the user access review process is an important part of meeting the requirements of INFOSEC4 and GOV2 under the PSR framework. Robust documentation allows agencies to review patterns in Infosec risk over time and address more strategic concerns to improve their security posture. The findings of user access reviews should also be used to inform the development or review of relevant internal policies, particularly information security policies and standard operating procedures within your organisation.

For more information about the information security standards you must meet, please refer to the following measures in the Protective Security Requirements and NZ Information Security Manual.

| | |
|---|---|
| **Protective Security Requirements**<br><br>• GOV2 (develop and maintain security policies and plans that meet your organisation's specific business needs)<br><br>• INFOSEC4 (keep your security measures up to date by maintaining access control systems) | https://protectivesecurity.govt.nz/governance/mandatory-requirements-2/<br><br>https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |
| **NZISM Chapter 5 (Information Security Documentation)**<br><br>• NZISM 5.2 Information Security<br>• NZISM 5.3 Security Risk Management<br>• NZISM 5.4 System Security Plans<br>• NZISM 5.5 Standard Operating Procedures<br>• NZISM 5.6 Incident Response Plans<br>• NZISM 5.7 Emergency Procedures<br>• NZISM 5.8 Independent Assurance Reports | https://www.nzism.gcsb.govt.nz/ism-document/#676 |

| | |
|---|---|
| **NZISM Chapter 16 (Access Control)**<br><br>• NZISM 16.1 Identification and Authentication<br>• NZISM 16.2 System Access<br>• NZISM 16.3 Privileged Access<br>• NZISM 16.4 Remote Access<br>• NZISM 16.5 Event Logging and Auditing | https://www.nzism.gcsb.govt.nz/ism-document/#1801 |

## Disabling access for ex-staff members

### Removing access to information systems for staff who have left the organisation

It is a mandatory requirement under the PSR framework to manage the departure of staff from your agency (PERSEC3). This requirement is in place to limit any risk to people, information and assets arising from people leaving your organisation. Your responsibilities under PERSEC3 include ensuring that any access rights, security passes, and assets are returned and that people understand their ongoing obligations.

Common ways that staff might retain systems access following their departure from an agency include:

- personal electronic devices previously used for work purposes that have not had their user access disabled
- agency owned electronic devices that have been sold or gifted to the departing staff member but have not had their user access disabled
- systems user accounts and passwords that have not been disabled.

**Risks**

Failing to disable user access for staff that have left the organisation may expose agencies to a number of risks including:

- staff gaining unauthorised access to restricted or sensitive information
- staff implementing unauthorised changes to data or systems, resulting in data corruption or loss
- information being replicated or distributed of outside of the network, resulting in data loss and potential breach of privacy or security protocols.

**Remember!**

Agencies are obligated to ensure that user access rights are disabled as soon as a staff member leaves the organisation and user access associated with security passes and assets (such as electronic devices) is also disabled.

The NZISM and the PSR framework provide additional details about what steps agencies must take to manage the departure of staff from their organisation effectively.

For more information about the information security standards you must meet, please refer to the following measures.

| | |
|---|---|
| **Protective Security Requirements**<br><br>• PERSEC3 (managing access rights, security passes and assets)<br><br>• INFOSEC4 (maintaining appropriate access to your information) | https://protectivesecurity.govt.nz/personnel-security/mandatory-requirements/<br><br>https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |
| **NZISM Chapter 16 (Access Control)**<br><br>• NZISM 16.1 Identification and Authentication<br>• NZISM 16.2 System Access<br>• NZISM 16.3 Privileged Access<br>• NZISM 16.4 Remote Access<br>• NZISM 16.5 Event Logging and Auditing | https://www.nzism.gcsb.govt.nz/ism-document/#1801 |
| **NZISM Chapter 21 (Working Offsite)**<br><br>• NZISM 21.1 Agency Owned Mobile Devices<br>• NZISM 21.4 Non Agency Owned Devices and Bring Your Own Device (BYOD) | https://www.nzism.gcsb.govt.nz/ism-document/#4450 |

# Change Management for Information Systems

## You need to manage changes to information systems to ensure that all changes are authorised and understood

Where a change to a system is likely to affect security settings, it is important that your agency has strong change management controls and processes in place. This will help to ensure the information held within the system remains adequately protected from unauthorised access.

It is essential to ensure there are also strong approval processes in place for all personnel requesting access to make changes within your systems, including employees, contractors and third parties. Regular auditing should be carried out on access to all systems to ensure that only authorised personnel can access information and systems in line with the specifications of their role.

**Risks**

Poorly managed system changes can expose your agency to a number of risks, including but not limited to:

- unauthorised changes
- unauthorised access to official information
- unplanned outages
- a low change success rate
- a high number of emergency changes
- delayed project implementations.[vii]

**Remember!**

Poor change management practices can affect the ability of your agency to deliver your business objectives. It is important that any changes to your information systems are authorised, properly documented and audited regularly to ensure issues (points of failure) are identified and addressed in a timely manner.

For more information about the information security standards you must meet, please refer to the following measures:

| | |
|---|---|
| **Protective Security Requirements**<br>• INFOSEC1 (understanding what you need to protect and the impact of any security breaches)<br>• INFOSEC3 (complete the | https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |

| | |
|---|---|
| certification and accreditation process to ensure your ICT systems have approval to operate)<br>• INFOSEC4 (maintaining appropriate access to your information + ensure that your information security remains fit for purpose)<br>- maintain access control systems and protect ICT equipment | |
| **NZISM Chapter 3 (Information Security Governance)**<br>• NZISM 3.4 (system owners)<br>• NZISM 3.5 (system users) | https://www.nzism.gcsb.govt.nz/ism-document#264 |
| **NZISM Chapter 6 (Information Security Monitoring)**<br>• NZISM 6.3 (change management) | https://www.nzism.gcsb.govt.nz/ism-document#738 |
| **NZISM Chapter 16 (Access Controls)**<br>• NZISM 16.1 (identification and authentication)<br>• NZISM 16.2 (system access)<br>• NZISM 16.3 (privileged access)<br>• NZISM 16.4 (remote access)<br>• NZISM 16.5 (event logging and auditing) | https://www.nzism.gcsb.govt.nz/ism-document#1801 |

## Review your information system policies

### You need to review information system policies to ensure they reflect the changing technology environment and to strengthen the governance of the organisation

Infosec policy is a key component of maintaining a strong information security posture within your agency and should include topics such as accreditation processes, personnel responsibilities, access control, emergency procedures and change management, among other things.[viii]

The technology environment is ever evolving and risks can emerge rapidly as new technologies are developed. While your Infosec policies may adequately address risks within the current environment, agencies should undertake regular risk assessments and document information security reviews of their systems at least annually to:

- identify any changes to the business requirements or concept of operation for the subject of the review
- identify any changes to the security risks faced by the subject of the review
- assess the effectiveness of the existing counter-measures
- validate the implementation of controls and counter-measures; and
- report on any changes necessary to maintain an effective security posture.

Annual reviews of an agency's information security posture will assist with ensuring that agencies are responding to the latest threats, environmental changes and that systems are properly configured, in accordance with any changes to information security documentation and guidance.

**Risks**

Failing to regularly review your Infosec policy could result in a changing risk tolerance for your organisation, which may expose your agency to vulnerabilities that could have previously been mitigated by regular review.

For more information about the information security standards you must meet, please refer to the following measures:

| | |
|---|---|
| **Protective Security Requirements**<br>• INFOSEC3 (confirm that your information security measures have been correctly implemented and are fit for purpose)<br>• INFOSEC4 (analyse evolving | https://protectivesecurity.govt.nz/information-security/mandatory-requirements-2/ |

| | |
|---|---|
| threats and vulnerabilities, keep your information security measures up to date, respond to information security incidents) | |
| **NZISM chapter 5 (Information Security Documentation)**<br>• NZISM 5.1 (documentation fundamentals)<br>• NZISM 5.2 (information security policies)<br>• NZISM 5.3 (security risk management plans)<br>• NZISM 5.4 (system security plans)<br>• NZISM 5.5 (standard operating procedures)<br>• NZISM 5.6 (incident response plans)<br>• NZISM 5.7 (emergency procedures)<br>• NZISM 5.8 (independent assurance reports) | https://www.nzism.gcsb.govt.nz/ism-document/#676 |
| **NZISM chapter 6 (Information Security Monitoring)**<br>• NZISM 6.1 Information Security Reviews<br>• NZISM 6.2 Vulnerability Analysis<br>• NZISM 6.3 Change Management | https://www.nzism.gcsb.govt.nz/ism-document/#738 |

*The NCSC can be contacted by email via incidents@ncsc.govt.nz or by phone on 04 498 7654. We encourage you to contact us at any time if you require any further assistance or advice.*

[i] NZISM 12.4.4.C.02
[ii] NZISM 12.4.4.C.03
[iii] NZISM 12.4.4.C.05
[iv] NZISM 12.4.4.C.06
[v] https://www.cyber.gov.au
[vi] https://www.cyber.gov.au/publications/restricting-administrative-privileges
[vii] UCISA/ITIL – A guide to change management (PDF), https://www.ucisa.ac.uk
[viii] NZISM 5.2.3.C.02