



# Information Security Manual

DECEMBER 2021

## Guidelines for System Management

### System administration

#### System administration of cloud services

System administration of cloud services brings unique challenges when compared to system administration of on-premise assets. Notably, responsibility for system administration of cloud services is often shared between service providers and organisations. As the technology stack and system administration processes implemented by service providers are often opaque to organisations, organisations should consider a service provider's control plane to operate within a different security domain. As such, the security controls below may require adjustment.

#### System administration processes and procedures

A key component of system administration is ensuring that privileged actions are performed using approved system administration processes supported by system administration procedures. This will ensure that privileged actions are undertaken in a repeatable and accountable manner.

**Security Control: 0042; Revision: 5; Updated: Dec-21; Applicability: All**

*System administration processes, and supporting system administration procedures, are developed and implemented.*

#### Separate privileged operating environments

One of the greatest threats to the security of a network as a whole is the compromise of the operating environment used for administration activities. Providing a separate privileged operating environment for privileged users, in addition to their unprivileged operating environment, provides greater assurance that privileged activities and credentials will not be compromised.

Using different physical machines is considered the most secure solution to separate privileged and unprivileged operating environments; however, a risk-based approach may determine that a virtualisation-based solution is sufficient. In such cases, the virtualised unprivileged operating environment should be run from within either a physical or virtualised privileged operating environment.

**Security Control: 1380; Revision: 5; Updated: Sep-21; Applicability: All**

*Privileged users use separate privileged and unprivileged operating environments.*

**Security Control: 1687; Revision: 0; Updated: Sep-21; Applicability: All**

*Privileged operating environments are not virtualised within unprivileged operating environments.*

**Security Control: 1688; Revision: 0; Updated: Sep-21; Applicability: All**

*Unprivileged accounts cannot logon to privileged operating environments.*

**Security Control: 1689; Revision: 0; Updated: Sep-21; Applicability: All**

*Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.*

**Security Control: 1381; Revision: 2; Updated: Sep-18; Applicability: All**

*Dedicated administrator workstations used for privileged tasks are prevented from communicating to assets not related to administrative activities.*

**Security Control: 1383; Revision: 2; Updated: Sep-18; Applicability: All**

*All administrative infrastructure including, but not limited to, administrator workstations and jump servers are hardened.*

## **Dedicated administration zones and communication restrictions**

Administration security can be improved by segregating administrator workstations from the wider network. This can be achieved a number of ways, such as via the use of Virtual Local Area Networks, firewalls, network access controls and Internet Protocol Security Server and Domain Isolation. It is recommended that segmentation and segregation be applied regardless of whether privileged users have physically separate administrator workstations or not.

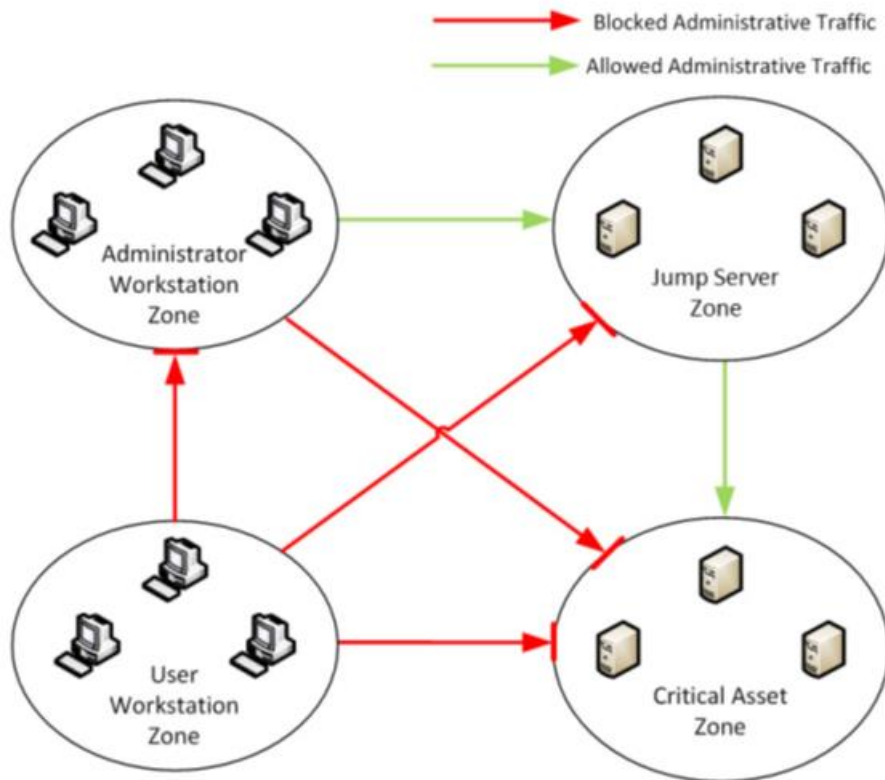
**Security Control: 1385; Revision: 2; Updated: Sep-18; Applicability: All**

*Administrator workstations are placed into a separate network zone to user workstations.*

## **Restriction of management traffic flows**

Limiting the flow of management traffic to only network zones explicitly required to communicate with each other can reduce the consequences of a network compromise and make it easier to detect if it does occur. Furthermore, although user workstations will have a need to communicate with critical assets such as web servers or domain controllers in order to function, it is highly unlikely that they will need to send or receive management traffic to these assets.

The following diagram outlines how management traffic filtering could be implemented between a network comprising different network zones. The only flows of management traffic allowed are those between the 'Administrator Workstation Zone' and the 'Jump Server Zone' as well as the 'Jump Server Zone' and the 'Critical Asset Zone'. All other traffic is blocked as there is no reason for management traffic to flow between the other network zones.



**Security Control: 1386; Revision: 4; Updated: Oct-19; Applicability: All**

*Management traffic is only allowed to originate from network zones that are used to administer systems and applications.*

## Jump servers

A jump server (also known as a jump host or jump box) is used to manage resources in a separate security domain. The use of jump servers as a form of management proxy can be an effective way of simplifying and securing privileged activities. Implementing a jump server can yield the following benefits:

- an efficient and effective focal point to perform multi-factor authentication
- a single place to store and patch management tools
- simplified implementation of management traffic filtering
- a focal point for logging, monitoring and alerting.

In a typical scenario, if a privileged user wanted to perform administrative activities they would connect directly to the target server using Remote Desktop Protocol or Secure Shell. However, in a jump server setup, the privileged user would first connect and authenticate to the jump server then use Remote Desktop Protocol, Secure Shell or remote administration tools to access the target server.

When implementing a jump server, it is recommended that organisations implement multi-factor authentication, enforce strict device communication restrictions and harden administrative infrastructure, otherwise a jump server will yield little security benefit.

**Security Control: 1387; Revision: 2; Updated: Sep-21; Applicability: All**

*Administrative activities are conducted through jump servers.*

**Security Control: 1388; Revision: 1; Updated: Sep-18; Applicability: All**

*Jump servers are prevented from communicating to assets and sending and receiving traffic not related to administrative activities.*

## Further information

Further information on the use of privileged accounts can be found in the access to systems and their resources section of the [Guidelines for Personnel Security](#).

Further information on multi-factor authentication for system administration can be found in the authentication hardening section of the [Guidelines for System Hardening](#).

Further information on network segmentation can be found in the network design and configuration section of the [Guidelines for Networking](#).

Further information on system administration can be found in the Australian Cyber Security Centre (ACSC)'s [Secure Administration](#) publication.

Further information on mitigating the use of stolen credentials can be found in the ACSC's [Mitigating the Use of Stolen Credentials](#) publication.

Further information can also be found in Microsoft's [Mitigating Pass-the-Hash \(PtH\) Attacks and Other Credential Theft Techniques, Version 1 and 2](#) publication.

## System patching

### Patching approaches

Patches for security vulnerabilities are provided by vendors in many forms, such as:

- fixes that can be applied to pre-existing application versions
- fixes incorporated into new applications or drivers that require pre-existing versions to be replaced
- fixes that require the overwriting of firmware on ICT equipment.

### When patches are not available

When patches are not available for security vulnerabilities there are a number of approaches that can be undertaken to reduce security risks. In priority order this includes resolving the security vulnerability, preventing exploitation of the security vulnerability, containing the exploitation of the security vulnerability or detecting exploitation of the security vulnerability.

Security vulnerabilities might be resolved by:

- disabling the functionality associated with the security vulnerability
- engaging a software developer to resolve the security vulnerability
- changing to different software or ICT equipment with a more responsive vendor.

Exploitation of security vulnerabilities might be prevented by:

- applying external input sanitisation
- applying filtering or verification on output
- applying additional access controls that prevent access to the security vulnerability
- configuring firewall rules to limit access to the security vulnerability.

Exploitation of security vulnerabilities might be contained by:

- applying firewall rules limiting outward traffic that is likely in the event of an exploitation
- applying mandatory access control preventing the execution of exploitation code
- setting file system permissions preventing exploitation code from being written to disk.

Exploitation of security vulnerabilities might be detected by:

- deploying a Host-based Intrusion Prevention System
- monitoring logging alerts
- using other mechanisms for the detection of exploits using the known security vulnerability.

## Patch management processes and procedures

Applying patches or updates is critical to ensuring the security of applications, drivers, operating systems and firmware in workstations, servers, mobile devices, network devices and all other ICT equipment. To assist in this, suitable sources of information should be monitored for information about new patches or updates.

**Security Control: 1143; Revision: 8; Updated: Dec-21; Applicability: All**

*Patch management processes, and supporting patch management procedures, are developed and implemented.*

**Security Control: 1493; Revision: 2; Updated: Jun-21; Applicability: All**

*Software registers are maintained and regularly audited for workstations, servers, mobile devices, network devices and all other ICT equipment.*

**Security Control: 1643; Revision: 0; Updated: Jun-21; Applicability: All**

*Software registers contain versions and patch histories of applications, drivers, operating systems and firmware.*

## When to patch security vulnerabilities

There are multiple information sources (such as news outlets, security researchers and vendors) that organisations can use to assess the applicability and impact of security vulnerabilities (such as if public exploit code is available or if the security vulnerability is already being exploited by an adversary) in the context of their environment.

Once a patch or update is released by a vendor, it should be applied in a timeframe that is commensurate with the likelihood of targeting by an adversary in the context of the organisation's environment. Doing so ensures that resources are spent in an effective and efficient manner by focusing effort on the most significant security vulnerabilities first.

If a patch or update is released for high assurance ICT equipment, the ACSC will conduct an assessment of the patch or update and may revise the ICT equipment's usage guidance. If a patch or update for high assurance ICT equipment is approved for deployment, the ACSC will inform organisations of the timeframe in which it is to be deployed.

If no patches or updates are immediately available for security vulnerabilities, vendor mitigations may provide the only effective protection until patches or updates become available. These vendor mitigations may be published in conjunction with, or soon after, security vulnerability announcements. Vendor mitigations may include disabling the vulnerable functionality within the operating system, application or device, or restricting or blocking access to the vulnerable service using firewalls or other access controls.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1692 and 1696 are not applicable.

**Security Control: 1690; Revision: 0; Updated: Sep-21; Applicability: All**

*Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.*

**Security Control: 1691; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.

**Security Control: 1692; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours if an exploit exists.

**Security Control: 1693; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.

**Security Control: 1694; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

**Security Control: 1695; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.

**Security Control: 1696; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within 48 hours if an exploit exists.

**Security Control: 1697; Revision: 0; Updated: Sep-21; Applicability: All**

Patches, updates or vendor mitigations for security vulnerabilities in drivers and firmware are applied within two weeks of release, or within 48 hours if an exploit exists.

**Security Control: 0300; Revision: 7; Updated: Sep-21; Applicability: S, TS**

High assurance ICT equipment is only patched or updated when approved by the ACSC using methods and timeframes prescribed by the ACSC.

## **How to patch security vulnerabilities**

To ensure that patches are applied consistently across an organisation's workstation and server fleet, it is essential that organisations use a centralised and managed approach. This will assist in ensuring the integrity and authenticity of patches being applied to workstations and servers.

**Security Control: 0298; Revision: 7; Updated: Oct-19; Applicability: All**

A centralised and managed approach is used to patch or update applications and drivers.

**Security Control: 0303; Revision: 6; Updated: Sep-18; Applicability: All**

An approach for patching or updating applications and drivers that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

**Security Control: 1497; Revision: 0; Updated: Sep-18; Applicability: All**

An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.

**Security Control: 1498; Revision: 1; Updated: Oct-19; Applicability: All**

A centralised and managed approach is used to patch or update operating systems and firmware.

**Security Control: 1499; Revision: 0; Updated: Sep-18; Applicability: All**

An approach for patching or updating operating systems and firmware that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.

**Security Control: 1500; Revision: 0; Updated: Sep-18; Applicability: All**



*An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.*

## Scanning for missing patches

To ensure that patches have been applied across an organisation's workstation and server fleet, it is essential that organisations scanning for missing patches on a regular basis. Ideally, vulnerability scanning should take place at half the frequency in which patches need to be applied. For example, if patches are applied fortnightly then vulnerability scanning should be undertaken weekly.

**Security Control: 1698; Revision: 0; Updated: Sep-21; Applicability: All**

*A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.*

**Security Control: 1699; Revision: 0; Updated: Sep-21; Applicability: All**

*A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.*

**Security Control: 1700; Revision: 0; Updated: Sep-21; Applicability: All**

*A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.*

**Security Control: 1701; Revision: 0; Updated: Sep-21; Applicability: All**

*A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.*

**Security Control: 1702; Revision: 0; Updated: Sep-21; Applicability: All**

*A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.*

**Security Control: 1703; Revision: 0; Updated: Sep-21; Applicability: All**

*A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in drivers and firmware.*

## Cessation of support

When applications, operating systems and ICT equipment reach their cessation date for support, organisations will find it increasingly difficult to protect against security vulnerabilities as patches, or other forms of support, will not be made available by vendors. While the cessation date for support for operating systems is generally advised many years in advance by vendors, other applications and ICT equipment may cease to receive support immediately after a newer version is released by a vendor.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security control 0304 is not applicable.

**Security Control: 1704; Revision: 0; Updated: Sep-21; Applicability: All**

*Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.*

**Security Control: 0304; Revision: 6; Updated: Sep-21; Applicability: All**

*Applications that are no longer supported by vendors are removed.*

**Security Control: 1501; Revision: 1; Updated: Sep-21; Applicability: All**

*Operating systems that are no longer supported by vendors are replaced.*

## Further information

Further information on patching evaluated products can be found in the evaluated product usage section of the [Guidelines for Evaluated Products](#).

Further information on patching security vulnerabilities can be found in the ACSC's [Assessing Security Vulnerabilities and Applying Patches](#) publication.

## Change management

### Identifying the need for change

The need for change can be identified in various ways, including:

- identification of security vulnerabilities or cyber threats
- users identifying problems or a need for system enhancements
- upgrades or patches for software or ICT equipment
- vendors notifying the end of life for software or ICT equipment
- the implementation of new software or ICT equipment
- organisational or business process changes
- other continuous improvement activities.

### Change management processes and procedures

The use of change management processes ensures that changes to systems are made in an accountable manner with appropriate consultation and approval. Furthermore, change management processes provides an opportunity for the security impact of any changes to systems to be considered.

In implementing changes to systems, it is important that change management procedures clearly articulate the steps to be taken for each part of change management processes.

**Security Control: 1211; Revision: 4; Updated: Dec-21; Applicability: All**

*Change management processes, and supporting change management procedures, are developed and implemented covering:*

- *identification and documentation of requests for change*
- *approval required for changes to be made*
- *assessment of potential security impacts*
- *notification of any planned disruptions or outages*
- *implementation and testing of approved changes*
- *the maintenance of system and security documentation.*



## Data backup and restoration

### Digital preservation policy

Developing and implementing a digital preservation policy as part of digital continuity planning can assist in ensuring the long term integrity and availability of important data is maintained. Especially when taking into account the potential for data degradation and media, hardware and software obsolesce.

**Security Control: 1510; Revision: 1; Updated: Aug-19; Applicability: All**

*A digital preservation policy is developed and implemented.*

### Data backup and restoration processes and procedures

Having data backup and restoration processes and procedures is an important part of business continuity and disaster recovery planning. Such activities will also form an integral part of an overarching digital preservation policy.

**Security Control: 1547; Revision: 1; Updated: Dec-21; Applicability: All**

*Data backup processes, and supporting data backup procedures, are developed and implemented.*

**Security Control: 1548; Revision: 1; Updated: Dec-21; Applicability: All**

*Data restoration processes, and supporting data restoration procedures, are developed and implemented.*

### Performing and retaining backups

When performing backups, all important data, software and configuration settings for software, network devices and other ICT equipment should be captured on a regular basis. This will ensure that should a system fall victim to a ransomware attack, important data will not be lost and that business operations will have reduced downtime.

Furthermore, to prevent backups from being retained for an insufficient amount of time to allow for the recovery of data, organisations are strongly encouraged to store backups for a sufficient period of time to meet business continuity requirements.

**Security Control: 1511; Revision: 2; Updated: Sep-21; Applicability: All**

*Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.*

### Backup access and modification

To mitigate the likelihood of data becoming unavailable due to accidental or malicious modification or deletion of backups, organisations should ensure that backups are sufficiently protected from unauthorised modification or deletion through appropriate access controls.

Note, for organisations implementing only Maturity Level Two of the [Essential Eight Maturity Model](#), security controls 1706 and 1708 are not applicable.

**Security Control: 1705; Revision: 0; Updated: Sep-21; Applicability: All**

*Unprivileged accounts, and privileged accounts (excluding backup administrators) cannot access other account's backups.*

**Security Control: 1706; Revision: 0; Updated: Sep-21; Applicability: All**

*Unprivileged accounts, and privileged accounts (excluding backup administrators) can't access their own account's backups.*

**Security Control: 1707; Revision: 0; Updated: Sep-21; Applicability: All**

*Unprivileged accounts, and privileged accounts (excluding backup administrators), are prevented from modifying or deleting backups.*

**Security Control: 1708; Revision: 0; Updated: Sep-21; Applicability: All**

*Backup administrators (excluding backup break glass accounts), are prevented from modifying or deleting backups.*

## Testing restoration of backups

To ensure that backups can be restored when the need arises, and that any dependencies can be identified and managed, it is important that restoration of systems, software and important data is routinely tested in a coordinated manner as part of disaster recovery exercises.

**Security Control: 1515; Revision: 2; Updated: Sep-21; Applicability: All**

*Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises.*

## Further information

Further information on business continuity can be found in the service continuity for online services section of the [Guidelines for Networking](#).

Further information on [preserving digital information](#) is available from the National Archives of Australia.