Whole-of-Government
Common Operating Environment
Policy
**Document Version Control**

<table>
<thead>
<tr>
<th>Document name</th>
<th>Project Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation:</td>
<td>Department of Finance and Deregulation</td>
</tr>
<tr>
<td>Project:</td>
<td>WofG COE</td>
</tr>
<tr>
<td>Document status:</td>
<td>Official Release</td>
</tr>
<tr>
<td>Version No:</td>
<td>3.0</td>
</tr>
<tr>
<td>File name:</td>
<td>WofG COE Policy v3.0.docx</td>
</tr>
<tr>
<td>Date:</td>
<td>24th May 2013</td>
</tr>
</tbody>
</table>

**Document Revision History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date of Issue</th>
<th>Author</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>26/11/2010</td>
<td>Mark Croonen</td>
<td>Initial Release</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coralie Volgyesi</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>5 April 2011</td>
<td>Leanne Chaplin</td>
<td>Update ISM Reference</td>
</tr>
<tr>
<td>2.0</td>
<td>13th December 2011</td>
<td>Leanne Chaplin</td>
<td>2011 Policy Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paul Ketelaar</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>12 June 2012</td>
<td>Nathan Watson</td>
<td>Update version history</td>
</tr>
<tr>
<td>3.0</td>
<td>24 May 2013</td>
<td>Leanne Chaplin</td>
<td>2012 Policy Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nathan Watson</td>
<td></td>
</tr>
</tbody>
</table>

**DOCUMENT OWNER:** Director, Common Operating Environment, Technology and Procurement Division.
# Table of Contents

- Common Operating Environment ................................................................. 4
- Introduction / Background ................................................................. 4
- Goals ........................................................................................................ 5
- Principles .............................................................................................. 5
- Composition ........................................................................................... 6
- Standards .............................................................................................. 7
- Application Management ......................................................................... 16
- Software Packaging ............................................................................... 16
- Security and User Configurations ......................................................... 17
- Logging ................................................................................................... 17
- Governance .......................................................................................... 18
- Understanding and Complying with the WofG COE Policy ..................... 18
- Related policies and initiatives ............................................................... 18
- Actions arising from policy breaches .................................................... 19
- Opt Out .................................................................................................. 19
- Exemptions ........................................................................................... 19
- Policy Implementation ........................................................................... 20
- Roles and Responsibilities in relation to the COE Policy ......................... 20
- COE Policy Review Cycle ....................................................................... 22
- SOE Implementation Roles .................................................................... 22
WHOLE OF GOVERNMENT COMMON OPERATING ENVIRONMENT POLICY

Common Operating Environment

Introduction / Background

1. To drive greater efficiency and transparency across Australian Government operations, the government has established a coordinated procurement contracting framework to deliver efficiencies and savings from goods and services in common use by Australian Government Departments and Agencies subject to the Financial Management and Accountability Act (FMA Act 1997).

2. The Whole of Government (WofG) Common Operating Environment (COE) was identified by the Desktop Scoping Study (Recommendation 2) as a critical element in driving future savings in services provisioning and increasing the flexibility and responsiveness of government operations.

3. In October 2009, the Government agreed to the development of a Whole of Government Common Operating Environment Policy. This policy is expected to:
   a. Optimise the number of desktop Standard Operating Environments (SOE) consistent with meeting the Government’s business objectives;
   b. Improve agency ability to share services and applications; and
   c. Support the Government’s e-Security Policy.

4. On October 16, 2009, the Secretaries’ ICT Governance Board (SIGB) approved the ICT Customisation and Bespoke Development Policy. Among other aims, this policy is expected to increase opportunities to standardise government business processes and systems.

5. The WofG COE Policy complements the ICT Customisation and Bespoke Development Policy by standardising and decreasing the number of desktop operating environments to be supported across Government. As of June 2010, there were a more than 186 separate SOE images built with different components, standards and technologies.
Goals

6. **Optimise the number of desktop SOE images**
   To meet the Government’s business objectives, defined common standards in hardware and software will reduce the number of SOE images required to support business needs. In turn, this will reduce the cost of SOE development and maintenance.

7. **Support the Government’s e-Security Policy**
   The COE will mandate a common desktop security configuration to be used across agencies; this will improve the level of security across agency networks. Industry partners will be provided with a consistent baseline to make application design more consistent across agencies and inherently more secure.

8. **Improve Agency ability to share services and applications**
   By using the agreed common standards, agencies will be able to share services and reduce the need for duplication. Lead agencies will be in a position to implement an application or service, which can then be reused by other government agencies.

9. The COE will enable agencies to respond more quickly to changing technology cycles, facilitating more cost-effective upgrades and supporting a move to more rapid adoption cycles, enhancing agency and government agility

Principles

10. The principles relate to the goals of the policy. They are enduring and should not require modification as technology changes.

11. Both the COE policy and principles are designed to be complementary to other policies. The COE Policy leverages principles defined by the cross agency services architecture\(^1\) and the Government’s principles for the Reuse of Software and other ICT Assets.

12. **Common and agreed standards**
    The COE will be based on common standards; where practical these will be based on open standards. Common standards will facilitate component reuse and the sharing of resources.

13. **Meets agency business requirements**
    The COE must be flexible enough to meet the requirements of all the agencies. It must also be capable of supporting multiple unique SOEs if there is a unique business requirement.

14. **Secure**
The COE must be secure on all levels and it must provide confidentiality, integrity and availability. Any procedures defined by the COE must have clear accountability and must be auditable. The COE Policy (subject to the Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF)) is applicable across all classification levels (e.g., unclassified through to Top Secret).

15. **Supportable**
All components used must be supportable to ensure the COE remains reliable and stable. Support must be readily available and cost efficient. The supporting skill sets must also be readily available.

16. **Complies with legislative requirements**
The COE will comply with all relevant legislative requirements.

**Composition**

17. The WofG Common Operating Environment is to be based on principles that are supported by the standards. The use of common standards promotes interoperability, provides common functionality and supports a consistent user experience. These standards will be applied to all SOEs regardless of how the desktop environment is delivered. E.g. Desktop, thin-client or desktop virtualisation.

18. The COE can accommodate multiple SOEs. The COE policy defines the principles and standards while the SOE identifies the solutions and technologies.

19. The COE principles and standards are documented as part of the policy. Each SOE will be built in accordance with platform specific build documentation, which will detail how the standards are instantiated for each platform.

20. A SOE is a specific solution based on the COE. It is comprised of an operating system, core services, a standard application set, a defined security configuration and a defined user configuration.
21. The **System** is defined as the layer of the SOE that the end user does not directly interact with, but is used to support the layers above such as the core services and standard applications.

22. **Core services** are services that are exposed to the user to perform a function, but do not manipulate or modify the user’s data.

23. **Standard applications** are generic applications which can be used to view, manipulate or save data.

24. Agency specific applications are used to deliver specific business needs. Agencies are responsible for the licensing and maintenance of these applications, as they are not considered part of the COE.

**Standards**

25. A component which is listed as ‘MANDATORY’ must be included in the SOE image and built in accordance with the platform specific build documentation.

26. Optional components do not have to be included in the SOE image but, if included, must be built in accordance with the platform specific build documentation.
27. Standards that use the term ‘must’ are mandatory requirements. Standards that use the term ‘should’ are strongly recommended.
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Standard</th>
<th>Effect</th>
</tr>
</thead>
</table>
| Configuration     | Security Configuration     | a. The Australian Government Information Security Manual (ISM) must be used for the selection of security controls for workstation operating systems.  
b. Security configurations from the platform specific build documentation must be centrally applied and managed. Any variations from the security configurations outlined in the SOE Build Guidelines must be managed using an appropriate risk management process. | a. Workstation operating systems are hardened appropriately.                                                                                                                                                                                     |
|                   | MANDATORY                 |                                                                                                                                             |                                                                                                                                                                                                        |
|                   | User Configuration        | a. Must support a consistent user experience regardless of the delivery mechanism  
b. All configurations should be in line with the best practice as defined in the platform specific guidelines  
c. Where possible the configuration must be centrally managed and not applied at the local system level  
d. Unnecessary functionality in the user interface is removed for the purpose of improving system performance.  
e. ICT green guidelines need to be taken into consideration in configuration of the user environment. | a. The modular build standards mean that the same user experience can be delivered regardless of whether the user is on a desktop or virtual client  
b. Where practical the user configuration will be defined in the platform specific guidelines to promote a consistent look and feel across agencies  
c. Agencies should seek to standardise on common user applications to promote a consistent user experience across the agencies  
d. The user configuration should support settings which reduce power consumption, such as the use of blank screen savers |
|                   | MANDATORY                 |                                                                                                                                             |                                                                                                                                                                                                        |
|                   | Multimedia Viewer         | a. The multimedia viewer must be capable of supporting at least one of the endorsed codecs.                                                                                                           | a. The multimedia viewer supports the preferred video and audio playback codecs.                                                                                                                                                   |
|                   | File Compression Utility  | a. Agencies should use the compression utility native to the operating system in use, or a product compatible with that utility.  
b. The compression utility should be configured to ensure that the ZIP file format is the default format.                                    | a. The operating system’s native compression utility, or a product compatible with that utility, is used for the compression/decompression of files and folders.  
b. Using the ZIP file format as the default format for the compression utility promotes compatibility between                                                                 |
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Standard</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>agencies using compression utilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDF Viewer</td>
<td>a. The PDF viewer must support the Open PDF file format as defined by ISO 32000-1:2008</td>
<td>a. The Open PDF file format is supported by the PDF viewer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internet Browser</td>
<td>a. The web browser must not allow users to install unauthorised add-ins or toolbars.</td>
<td>a. Users are not able to configure their browsers by installing unapproved add-ins or toolbars.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Communications Client</td>
<td>a. The communications client must support the POP3, POP3S, IMAP, IMAPS, SMTP and SMTPS protocols.</td>
<td>a. All common email protocols, and their secure implementations, are supported by the communications client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. The communications client must support shared calendars and contacts</td>
<td>b. Users are capable of viewing shared calendars and contacts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. The communications client must support the use of PKI certificates for signing and encrypting email.</td>
<td>c. Emails can be encrypted and signed using PKI certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>d. The communications client must support the use of an email protective marking solution.</td>
<td>d. Protective markings can be applied to all emails.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e. Communications clients should be configured to view emails in plaintext mode.</td>
<td>e. Viewing emails in plaintext mode protects against emails being used as a vector for active content attacks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office Productivity Suite</td>
<td>a. The office productivity suite must support at least version 1.1 of the Open Document Format for Office Applications (ODF) as defined by ISO/IEC 26300:2006/Amd 1:2012.</td>
<td>a. Office productivity suites provide support for a common file format to facilitate the exchange of information between agencies. This does not preclude the use of other file formats.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VPN Client</td>
<td>a. The VPN client must meet the minimum cryptographic assurance requirements of the Australian Government Information Security Manual.</td>
<td>a. The VPN client provides sufficient assurance in the protection of sensitive or classified information when in transit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. The VPN client must use multi-factor authentication where possible.</td>
<td>b. Multi-factor authentication provides additional protection against malicious code capturing</td>
</tr>
<tr>
<td>Category</td>
<td>Component</td>
<td>Standard</td>
<td>Effect</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Antivirus             | MANDATORY                                     | a. The antivirus client must prevent end users stopping the service.  
b. The antivirus client must automatically and transparently report scanning results.  
c. The antivirus client must be configured to provide the maximum level of protection afforded by the selected product. | a. Users are unable to disable or bypass the antivirus client.  
b. Scanning reports are automatically reported rather than asking users for permission to report results.  
c. The maximum protection afforded by the antivirus client is applied.                                           |
| Firewall              | MANDATORY                                     | a. The firewall client must prevent users from stopping the service.  
b. The firewall client must be capable of preventing unauthorised inbound and outbound connections at the application layer.  
c. The firewall client must be able to change its configuration automatically based on location. | a. Users are unable to disable or bypass the firewall.  
b. Network connections are able to be managed from the application level rather than by filtering on only the address and port. For example iexplore.exe should be allowed to communicate out to <address>:80 rather than just allowing any application to communicate out to <address>:80.  
c. The firewall client is able to automatically configure itself based on the current connection and type of network to which the device is connected. |
| Host Based Intrusion  | In Intrusion Prevention Client                | a. The host-based intrusion prevention client must prevent users from stopping the service.  
b. The host-based intrusion prevention client must automatically and transparently report scanning results.  
c. The host-based intrusion prevention client must be configured to provide the maximum level of protection afforded by the selected product. | a. Users are unable to disable or bypass the host-based intrusion prevention client.  
b. Scanning reports are automatically reported rather than asking users for permission to report results.  
c. The maximum protection afforded by the host-based intrusion prevention client is applied. |

Usernames and passwords.
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Standard</th>
<th>Effect</th>
</tr>
</thead>
</table>
| Application Whitelisting Client | MANDATORY                         | a. The application whitelisting client must prevent users from stopping the service.  
b. The application whitelisting client should use hashes of approved executables, and if possible approved DLLs, rather than approved directories. | a. Users are unable to disable or bypass the application whitelisting client.  
b. Only specifically approved executables are allowed to execute on workstations.                                                                                                                                                                                                 |
| Desktop Management Client |                                  | a. The desktop management client must support remote desktop connectivity for support staff.  
b. The desktop management client must support notification of active remote desktop sessions.  
c. The desktop management client must have the ability to collect asset/configuration information. | a. Support staff are able to remotely troubleshoot and rectify issues with workstation operating systems.  
b. Users can be notified and requested to authorise third party access to their desktop sessions.  
c. Workstation asset and configuration information is made available to support staff.                                                                                                                                 |
| Email Classification Tool |                                  | a. Must support the [Australian Email Protective Marking Standard](#). | a. Emails have a protective marking indicating the classification and/or sensitivities associated with its content.                                                                                                                                                                                                                       |
| End Point Security Client |                                  | a. The endpoint device control client must prevent users from stopping the service.  
b. The endpoint device control client must support the disabling of external ports such as USB, eSata or Firewire, Express Card and Thunderbolt to selected user groups.  
c. The endpoint device control client must support the disabling of optical drives for both read and write.  
d. The endpoint device control client must support the prevention of unauthorised installation of USB devices such as scanners, smartphones, cameras and mass storage devices such as thumb drives and external hard drives. | a. Users are unable to disable or bypass the endpoint device control agent.  
b. Communications ports that pose a security risk to operating systems are disabled if not required by a specific user group.  
c. Access to optical drives can be controlled.  
d. Devices that pose a security risk to operating systems or permit the exfiltration of sensitive data can be controlled from working with operating systems. |
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Standard</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>The System</td>
<td>Encryption Client</td>
<td>a. The encryption client must meet the minimum cryptographic assurance requirements of the <em>Australian Government Information Security Manual</em>.</td>
<td>a. The encryption client provides sufficient assurance in the protection of sensitive or classified information when at rest.</td>
</tr>
</tbody>
</table>
|               | Codec Pack        | a. The codec pack must support a codec capable of video playback as defined by the MPEG-4 part 2 standard.  
                     b. The codec pack must support a codec capable of audio playback as defined by the MPEG-1 or MPEG-2 Audio Layer 3 standard.                                                                                       | a. When developing new applications or upgrading legacy applications endorsed codecs are used to promote interoperability.                                                                                                                                                          |
|               | Application       | a. Applications should only have a requirement for an N-1 application framework.  
                     b. Legacy applications with a need for an application framework outside of N-1 should have the required framework deployed as a part of the application.                                                                                       | a. Only applications that use an N-1 application framework are deployed on systems.  
                     b. Legacy applications which have a need for an older framework outside of N-1 should have the required framework deployed as part of the application and not as part of the operating system.                                                                                       |
|               | Frameworks        |                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                            |
| Storage       | MANDATORY         | a. Sensitive or classified information should not be stored on local workstations; however, if unavoidable it must be appropriately encrypted.  
                     b. Sensitive or classified information stored on portable devices must be encrypted.  
                     c. Local caching of network-stored user profiles should be used.                                                                                       | a. Sensitive or classified information is either stored on network shares or appropriately encrypted on local workstations.  
                     b. Sensitive or classified information on portable devices is appropriately encrypted.  
                     c. Local caching of network-stored user profiles is used, where practical, to provide a consistent experience for users regardless of which workstation they use.                                                                                       |
| Operating     | MANDATORY         | a. The operating system must be procured in accordance Commonwealth Procurement Guidelines and in accordance with Whole-of-Government ICT policies including the ICT Customisation and Bespoke | a. Compliance with the Commonwealth Procurement Rules is maintained.  
                     b. The enhanced security available in the 64 bit versions of operating systems is utilised.                                                                                                                               |
<table>
<thead>
<tr>
<th>Category</th>
<th>Component</th>
<th>Standard</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Development Policy.</td>
<td>c. Agencies employ a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. The 64 bit (X64) version of the operating system must be used.</td>
<td>d. Vulnerabilities in operating systems and applications are addressed as soon as possible through the remote deployment of patches without the need for end-user interaction.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>c. Agencies must adhere to effective patching policies and take into account system importance, patch testing and patch criticality as specified in the ISM.</td>
<td>e. All applications deployed on operating systems are approved by an appropriate Agency authority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>d. Patches for the operating system and applications must be able to be deployed remotely without interaction from end users.</td>
<td>f. Where possible, applications are deployed using an automated process to ensure consistent configuration throughout an environment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e. All applications deployed on the operating system must be approved by the agency.</td>
<td>g. Applications are installed in defined locations, for example, in Program Files, not in a user’s home directory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>f. Agency approved applications should support automated deployment.</td>
<td>h. Applications are managed in an efficient and consistent manner.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>g. Deployed applications must be installed in defined locations only on the operating system.</td>
<td>i. Vendor support is available for Commercial Off-The-Shelf (COTS) applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>h. Applications should be centrally administered and updated.</td>
<td>j. Users are prevented from executing arbitrary or malicious software or bypassing application whitelisting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>i. Applications should be vendor supported.</td>
<td>k. User access is limited to the minimum necessary level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>j. Users must not have write permission to directories that software is executed from.</td>
<td>l. Multi-factor authentication provides additional protection against malicious code capturing usernames and passwords.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>k. Users must not have the ability to manually install unapproved applications, uninstall applications or disable security functionality.</td>
<td>m. Data Execution Prevention (DEP) is utilised for all compatible programs and services to assist in mitigating operating system exploits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>l. Multi-factor authentication must be supported.</td>
<td>n. Address Space Layout Randomisation (ASLR) is utilised to assist in mitigating operating system exploits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>m. Data execution prevention (DEP) must be enabled for essential programs and services, preferably all programs and services with incompatible applications opting-out.</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Component</td>
<td>Standard</td>
<td>Effect</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>----------</td>
<td>--------</td>
</tr>
</tbody>
</table>
|          | p.        | Functionality allowing the automatic execution of files on removable media and devices must be disabled. | o. The likelihood of passphrase hashes being compromised is reduced.  
|          |           | p. Infection resulting from the automatic execution of malicious files contained on removable media and devices is prevented. |  
|          |           |          |        |
|          |           |          |        |
|          | b.        | Support for IPv6 on network interfaces must be disabled until it is ready to be deployed across the network infrastructure. | a. Applications and network interfaces support IPV6.  
|          |           |          | b. Enabling IPv6 without proper support on the network infrastructure does not expose workstations to unnecessary security risks. |
|          |           |          |        |
| Hardware | a.        | All hardware must comply with minimum specifications as outlined by the Desktop Hardware panel.  
|          | b.        | Hardware must support the Green ICT guidelines.  
|          | c.        | Hardware should have a Trusted Platform Module (TPM).  
|          | d.        | Hardware must support 64bit operating systems.  
|          | e.        | Hardware must support Wake-on-LAN functionality. | a. All desktops are procured in accordance with the WofG Desktop Hardware panel, which includes the appropriate driver software to suit the SOE.  
|          |           |          | b. All desktops support the Green ICT guidelines.  
|          |           |          | c. TPMs are used where available for the generation and storage of cryptographic material used by the operating system.  
|          |           |          | d. The 64bit (x64) version of the operating system can be used on the hardware.  
|          |           |          | e. Workstations can be woken from Sleep mode across the network to facilitate the application of security patches. |
|          |           |          |        |
Application Management

28. To maintain consistency and reduce complexity, all applications used as part the COE (the System, Core Services and Standard Applications) must be the current and supported version (known as N) or its immediate predecessor (known as N-1). N refers to the major version of an application, e.g. version 2.x is N, version 1.0 or 1.1 are N-1. This will ensure all applications are supported and by allowing the N-1 version gives the agency flexibility to plan required upgrades.

29. Support for existing or legacy applications should be structured so dependencies such as codecs and application frameworks are tied to the application and not the SOE. This will support a modular design of the SOE and ensure that the SOE can be maintained in accordance with the N-1 application management principle. To support the modular design agencies should consider the use of virtualisation to decouple legacy applications from the SOE. The form of virtualisation best suited for an agency will be dependent on factors such as the infrastructure and the network bandwidth available.

30. As the agencies converge on the COE standards, it is expected that the need for the virtualisation of legacy applications will be reduced.

31. To ensure the desktop environment remains consistent, application updates should be pushed by a centrally managed distribution mechanism. Applications which are installed on the desktop should not be configured to pull updates from external sources, such as vendor websites. Client based update services such as these should be disabled or not installed. The updating of anti-virus signatures or configuration files is not considered to be an application update.

32. To facilitate application white listing where possible, applications must be installed in the locations as detailed in the specific system build documentation for each platform.

33. Application Whitelisting must be used to help prevent unapproved applications from running.

34. Applications should support the use of roaming user profiles.

Software Packaging

35. To support the goal of agencies being able share services, the packaging of software should be managed so an application can be packaged once and reused many times. Agencies should look to use application virtualisation to achieve this. Virtualisation may reduce the number of distribution methods required and make it possible for agencies to share packaged applications.
Security and User Configurations

36. All standard products will have defined security configurations based on ASD’s and the vendor’s recommendations. Configuration settings will be specified by Finance and endorsed by ASD.

37. The security and user configurations for each operating system platform will be detailed in the specific system build documentation for each platform and marked as ‘mandatory’. This will represent the minimum requirements for the environment with agencies able to add configurations to meet their requirements.

38. Agency specific security and end user configurations may be applied on top of the COE configurations; however, they must not decrease or weaken the level of security provided by the base COE configurations.

Logging

39. To ensure legal and security requirements are met in accordance with the ISM and NAA “Administrative Functions Disposal Authority, Technology and Telecommunications” policy, Agencies must have a logging policy which clearly defines:
   a. what events they capture
   b. why the events need to captured
   c. how long the logs will be stored for

40. Log details should include:
   a. date/time of event
   b. user details
   c. workstation details
   d. event message and relevant details

41. Logs should be kept for the following categories:
   a. security configuration
   b. anti-virus, firewall
   c. desktop management
   d. end point security
   e. operating system functions to include:
      o privileged operations and access
      o log on/log off events
      o failed authentication attempts
      o system/application security alerts.

42. To ensure data integrity, Agencies should use a configuration of either remote logging or the transfer of local event logs to a central server. The use of centralised logging does not preclude the logs also remaining resident on their local systems.
Governance

Understanding and Complying with the WofG COE Policy

43. This Policy applies to all FMA Act Agencies. It is also available to Commonwealth Authority and Companies (CAC) Act Agencies and the States and Territories.

44. It is the responsibility of all FMA Act Agencies to ensure they understand and comply with this Policy.

45. Agencies must ensure their environment remains compliant with the policy as published at the time it was developed. Agencies must also remain compliant with future releases of the policy.

46. Compliance with the COE standards will be monitored and conducted by Agencies, with these results to be incorporated into the Finance annual benchmark reports.

Related policies and initiatives

47. The COE policy is supported by and complements the following policies and initiatives:

a. Section 44(1) of the Financial Management and Accountability Act 1997 (FMA Act) requires all Government Departments to use available resources in an efficient, effective and ethical manner.

b. "Strategies to Mitigate Targeted Cyber Intrusions". This policy addresses the top four priorities identified in this list and several others.

c. The COE policy addresses the first requirement of the governance requirements as identified in schedule 1 of the ICT Customisation and Bespoke Development policy.

d. Process for Administration of Opt-Outs from Whole-of-Government Arrangements


f. Green ICT guidance list, the COE will support the Green ICT guidance list. All SOE images built in accordance with the COE policy must implement the relevant configuration settings as outlined in the Green ICT guidance list.

g. National Security Information Environment Roadmap, the COE policy provides common standards to deliver a secure desktop environment and promotes interoperability between agencies.

Actions arising from policy breaches

48. Agencies assessed as non-compliant with COE Policy will be identified in annual reporting to the Secretaries ICT Governance Board (SIGB). The Chairperson of SIGB may, where warranted, raise the issue of non-compliance with the relevant Agency head for further action.

Opt Out

49. This policy is subject to the process for administration of opt-outs from Whole-of-Government arrangements.

50. Initial opt-out considerations will be factored into the transition plan and are expected to show how alignment to the policy will be achieved as part of the transition plan. Claims for opting out will not be considered during the transition phase.

51. When seeking an opt-out, an agency will need to include a remediation plan to detail how it will return to the WofG COE policy. Opt-outs are limited to a maximum of 3 years, after which the original business case will be reassessed to ensure it is still valid.

52. While it is recognised that agencies may have a need to develop separate SOE images, it is expected that these images will comply with the standards set out for the COE to ensure that agencies can still share data and services in a seamless manner.

Exemptions

53. This Policy is directed at general-purpose systems such as managed desktops and laptops. Embedded computers, process control systems or specialised scientific systems are outside the scope of this policy.

54. Modifications to these exempted systems are to be minimal and they should only deviate from the COE to the extent required to make the device or application functional.

55. Agencies are not required to seek an opt-out for exempted systems as they are automatically excluded from the policy. As part of their annual benchmark reporting, agencies will need to report on the number of excluded systems, the reason for their exclusion and modifications made to the system.

56. All excluded systems are still required to meet security standards as defined in the Information Security Manual (ISM).

57. Agencies may make changes to mandatory security configurations in order to support a critical agency need. In doing so, agencies must
• develop a risk assessment covering the required change(s), including appropriate risk reduction strategies, for acceptance through the agency’s risk management framework.
• maintain a record of any change(s) to the configuration baseline.
• inform Finance as soon as practical of the change(s), providing a brief business case and details of the risk assessment.

Agencies must manage non-compliance with relevant ISM controls separately from changes to the configuration baseline.

Policy Implementation

58. The standards endorsed by this policy come into effect when an agency is ready to deploy a new version of their base SOE. At this time agencies will need to follow their normal application testing regimes and build the SOE in accordance with the standards endorsed by this policy.

59. A new version of the SOE is considered to be an upgrade of the operating system or the deployment of a substantial update such as the release of a service pack.

60. Agencies may choose to integrate aspects of this policy prior to an operating system upgrade and are encouraged to be proactive where ever possible.

Roles and Responsibilities in relation to the COE Policy

61. Finance:
   a. All WofG COE Policy instantiation activities. These include:
      o Coordinate, develop and publish the WofG COE Policy
      o Coordinate, develop, build and test the Windows7 SOE (pilot activity)
      o Coordinate, develop and publish the WofG COE Policy Transition Plan
      o Identification of potential WofG software licence options
      o Identification of reporting metrics and inclusion in annual benchmarking activities

   b. Ongoing management and maintenance of the WofG COE Policy, the supporting SOEs and related documentation sets. This includes:
      o Annual reviews of the COE Policy, covering:
        ▪ Coordinating requests for change for the WofG COE Policy
        ▪ Coordinating policy change request reviews
        ▪ Understanding the security implications associated with change requests
        ▪ Testing of proposed baseline configuration changes
        ▪ Recommending changes
        ▪ Updating COE Policy, baseline configuration and documentation as required
        ▪ Publishing updates
      o Identification of SOE standard software with WofG licensing potential
Coordination of compliance audits and reporting
Endorsement of security configuration and ongoing changes to the security baseline (including security configuration exception/ issues resolution)
Management and maintenance of the SOE documentation sets and images
Provision of policy advice and guidance
Availability of baseline configuration and supporting documentation
Programming of COE Policy and baseline configuration updates
Review of Desktop Hardware panel specifications in conjunction with panel hardware updates

62. WofG COE Working group
   a. Assist and support Finance in managing and maintaining the WofG COE Policy. This includes:
      o Definition of COE standards and composition
      o Endorsement of WofG COE Policy and supporting SOE documentation sets
      o Annual review of WofG COE Policy and SOE image requests for change

63. Government Agencies:
   a. Ensuring business specific applications work within the specifications of the COE
   b. Providing feedback to Finance on any COE Policy or SOE image related issues (including security configuration settings)
   c. Ensuring policy compliance (including security configurations) is maintained on their networks
   d. Initiating a COE Policy Opt Out request where appropriate
   e. Programming and scheduling of agency upgrades
   f. Inform Finance of any emergency changes to the configuration baseline
   g. Provide data as required for the reporting metrics

64. SIGB/CIOC
   a. Endorsement and approval of the COE policy and supporting SOE documentation sets
   b. Review of recommended opt out requests

65. ASD
   a. Review and endorsement of COE security configurations and any proposed changes to the COE security configuration baseline
   b. Assist Finance with assessing the security impact of any opt out requests to include
      o Identification of unacceptable risk
      o Identification of acceptable risk mitigation methods

66. Lead Agency
   a. Lead Agencies may be identified to assume some of the Finance responsibilities. These may include:
      o Management and maintenance of the SOE documentation sets and images
      o Testing of proposed SOE changes
      o Review and maintenance of SOE images
      o SOE image performance monitoring
Testing of SOE images against recommended hardware specifications as defined by the Desktop Hardware procurement panel.

**COE Policy Review Cycle**

67. The COE standards will be reviewed annually, starting with a call for change requests from agencies in July each year. Requests for changes can be based on business or technology requirements.

68. This will be followed by a two month review period of the requested changes starting in August. The review will be lead by Finance and supported by members of the COE working group.

69. The COE standards and the SOE documentation sets will then be revised from October with updates to be released in December.

<table>
<thead>
<tr>
<th>WofG Common Operating Environment Policy Review</th>
<th>Finance</th>
<th>COE WG</th>
<th>Agencies</th>
<th>SIG/CIOC</th>
<th>ASD</th>
<th>Lead Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>COE Policy requests for change identified</td>
<td>A/R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>COE Policy changes reviewed</td>
<td>A/R</td>
<td>R</td>
<td>C/I</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Security implications of changes understood and endorsed</td>
<td>A/R</td>
<td>C</td>
<td>C/I</td>
<td>R</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Recommended changes tested against baseline configuration</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Recommended changes agreed</td>
<td>A/R</td>
<td>R</td>
<td>C/I</td>
<td>I</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Baseline configuration and documentation updated</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Changes approved</td>
<td>A/R</td>
<td>C</td>
<td>I</td>
<td>R</td>
<td>I</td>
<td>I</td>
</tr>
<tr>
<td>Update COE Policy, baseline configuration and documentation published</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>

- **Responsible:** person who performs an activity or does the work.
- **Accountable:** person who is ultimately accountable and has Yes/No/Veto.
- **Consulted:** person that needs to feedback and contribute to the activity.
- **Informed:** person that needs to know of the decision or action.

**SOE Implementation Roles**

70. Agencies are responsible for all programming and scheduling activities related to their operating system upgrades. Finance will provide advice and guidance and access to the SOE images and associated documentation. Testing of business applications is an agency responsibility. Any issues that would require a change to either the COE Policy or SOE image or supporting documentation are to be reported to Finance.
<table>
<thead>
<tr>
<th>WofG Common Operating Environment</th>
<th>Finance</th>
<th>COE WG</th>
<th>Agencies</th>
<th>SGB/CIOC</th>
<th>ASD</th>
<th>Lead Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>COE Policy advice and guidance</td>
<td>A/R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SOE documentation and image availability</td>
<td>A/R</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Programming of Agency SOE upgrades</td>
<td>C/I</td>
<td>A/R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensuring COE Policy compliance</td>
<td>C/I</td>
<td>A/R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing and management of agency business applications</td>
<td>I</td>
<td>A/R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initiation of opt out requests where appropriate</td>
<td>C/I</td>
<td>I</td>
<td>A/R</td>
<td>C/I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting COE Policy or baseline configuration issues</td>
<td>C/I</td>
<td>I</td>
<td>A/R</td>
<td>C/I</td>
<td>I</td>
<td></td>
</tr>
</tbody>
</table>

- **Responsible**: person who performs an activity or does the work.
- **Accountable**: person who is ultimately accountable and has Yes/No/Veto.
- **Consulted**: person that needs to feedback and contribute to the activity.
- **Informed**: person that needs to know of the decision or action.