Australian Government
Department of Finance and Deregulation

Whole-of-Government
Common Operating Environment (COE)

SOE Build Guidelines – Windows 7 Enterprise with SP1 x64

Document Version Control

Document name	***Project Plan***
Organisation:	Department of Finance and Deregulation
Project:	WofG COE
Document status:	~~Official Release~~Draft
Version No:	3.0~~2.1~~
File name:	SOE Build Guidelines – Windows v3.0 – Official Draft ~~v2.1~~.docx
Date:	~~12~~24th ~~June~~May 2013~~2~~

Document Revision History

Version	***Date of Issue***	***Author***	***Reason for Change***
1.0	26/11/2010	G. Noack	Initial Release
2.0	19/12/2011	P. Ketelaar	2011 Review
2.1	12/6/2012	N.Watson	Update version history
3.0	24/5/2013	L. Chaplin N. Watson	2012 Review

DOCUMENT OWNER: Director, Common Operating Environment, ~~Agency Services~~Technology and Procurement Division.

Table of Contents

1. Introduction

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).

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.

In October 2009, the Government agreed to the development of a Whole of Government Common Operating Environment Policy. This policy is expected to:

- Optimise the number of desktop Standard Operating Environments (SOE) consistent with meeting the Government's business objectives;
- Improve Agency ability to share services and applications; and
- Support the Government's e-Security Policy.

On October 16, 2009, the Secretaries ICT Governance Board (SIGB) approved the ICT Customisation and Bespoke Development Policy, which strengthens the governance of customised and bespoke development. Among other aims, this policy is expected to increase opportunities to standardise government business processes and systems.

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 more than 186 separate SOE images built with different components, standards and technologies.

The Windows SOE is the practical implementation of the WofG COE Policy for the Microsoft Windows platform.

2. Common Software Installation Principles

All software installations are to be completed in accordance with the following common software installation principles:

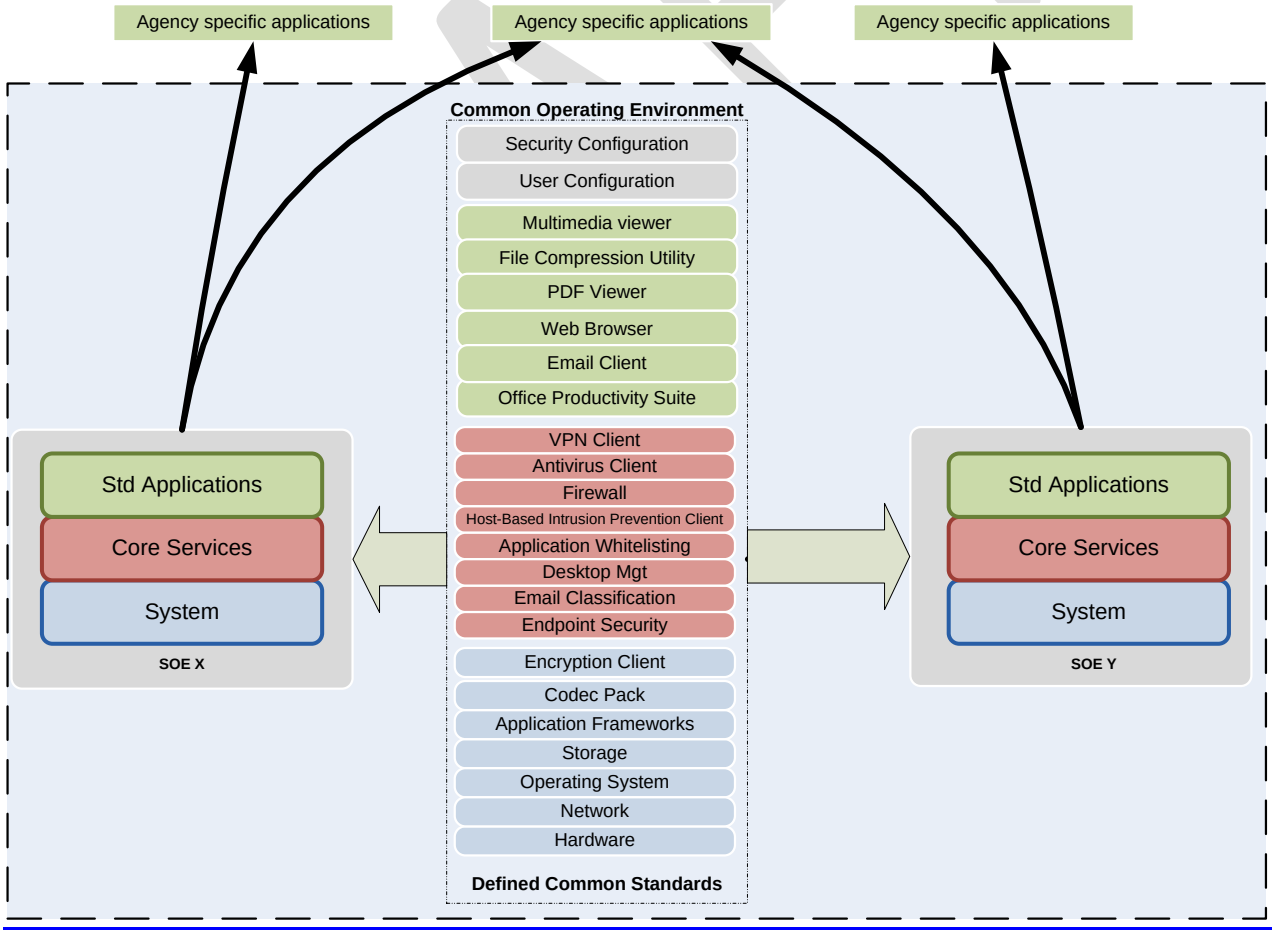
1. Installations are to be completed to an appropriate location within the "Program Files" or "Program Files (x86)" directory, typically "C:\Program Files\<Vendor>\<Product>" or "C:\Program Files\<Product>".
2. Applications should make use of the operating systems settings for localisation options. Where product localisation is necessary, applications should be localised for Australia, using the US keyboard.
3. Agencies are to determine whether to allow software update services to be installed. ~~Software update services are not to be installed. Where this is not possible, remedial action to disable them and remove registry entries or short cuts that launch them is to be~~

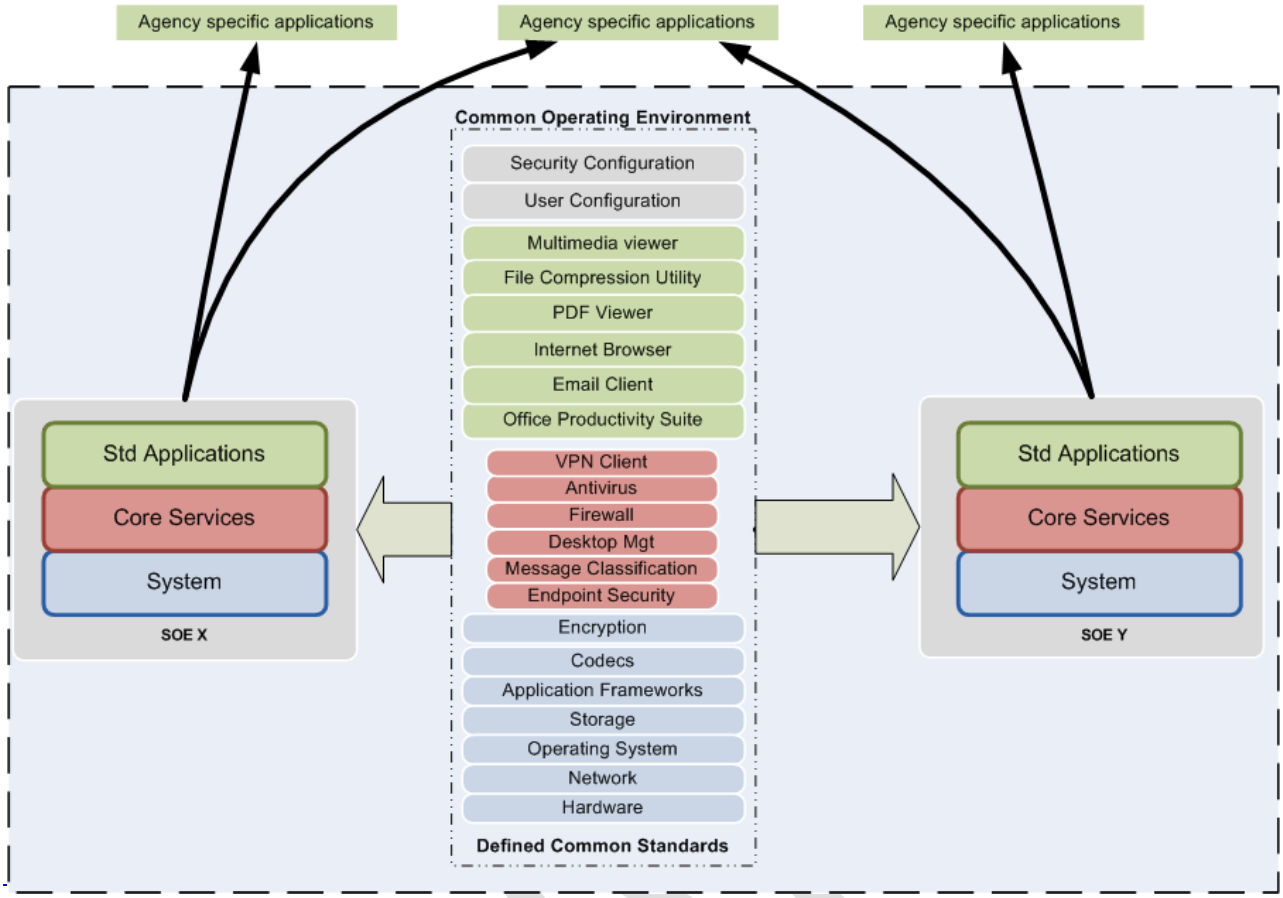
~~taken. This requirement does not apply where the software updating is an essential part of the "service" being provided by the application, e.g. Anti-Virus software.~~

4. Do not install any form of "value adding" software, such as browser toolbars or helpers, unless they are explicitly required. Where they are automatically installed, but not required, take remedial action to remove or permanently disable them.
5. To be compliant with the WofG COE Policy, the approved product, as listed in this document, is to be installed for each component. Unless otherwise stated, additional products may be installed for a specific component, provided that the additional products are also fully compliant with the relevant standards.
6. Persistent configuration settings, including security configuration settings, are to be managed centrally and enforced. In most Windows environments, this will be achieved using networked based policies, such as the Group Policy feature of Microsoft Active Directory.

3. Build Components

The Windows SOE is constructed using a modularised approach, and is comprised of multiple components as depicted in the following diagram:





The standards, product selection, and configuration requirements associated with each component are defined in the following sections. The configuration settings are documented in full in the applicable Annexes to this document.

3.1. Security Configuration

The Security Configuration is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
a. The *Australian Government Information Security Manual* (ISM) must be used for the selection of security controls for workstation operating systems. ~~a.~~b. Group policies from the *SOE Build Guidelines – Windows 7 Enterprise with SP1 x64* must be centrally applied and managed. Any variations must be managed using an appropriate risk management process.~~Workstations should be configured to ensure software, Operating System components and hardware functionality or features are removed or disabled.~~ ~~b. By default, users are not to have accounts which grant them privileged access to the system. Privileged access to systems must be granted in~~	a. Workstation operating systems are hardened appropriately. ~~Workstations are to be hardened in accordance with the Software Security Section in the ISM Controls Manual. The Privileged Access Section of the ISM Controls Manual defines privileged access and supports the use of separate accounts where privileged access is required.~~ ~~The security configurations will be specified by AGIMO and endorsed by DSD~~

Standard	Effect
accordance with the ISM c. Where possible, the configuration must be centrally managed and not applied at the local system level d. The configuration must be endorsed by DSD e. Must support *Logging* as defined in the WofG COE Policy f. The application of security patches or other security maintenance activities must take precedence over energy saving considerations Must support centralised operating system patching	

Where security configurations are not covered by the ISM, agencies should refer to appropriate hardening guides, including those published by DSD and by vendors.

Mandatory security configurations as documented at Annex A and Annex K.

3.2. User Configuration

The User Configuration is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
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. Access to data should be done with the use of links to a network path with reference to mapped networked drives to be avoided d. Where possible the configuration must be centrally managed and not applied at the local system level e. The interface should be minimal to reduce the impact on system performance f. 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. Users should not need to know about mapped network drives (if used), they should be able to go to a standard icon in a standard location to access their personal or shared data d. Agencies should seek to standardise on common user applications to promote a consistent user experience across the agencies e. The user configuration should support settings which reduce power consumption, such as the use of blank screen savers

Recommended user configurations as documented at Annex B.

3.3. Power Usage Policy

The Power Usage Policy is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
a. ICT green guidelines must be taken into	a. The power consumption of inactive

Standard	Effect
consideration in the configuration of workstation operation systems.	workstations is reduced by automatically turning off monitors and putting workstations to sleep.

In conjunction with power saving settings, systems should be configured with a session/screen lock, as documented at Annex B, to prevent unauthorised access to a system to which an authorised user has already been authenticated.

Mandatory security configurations as documented at Annex M.

~~3.2.1. Screen Saver Settings~~

~~The use of screen savers will be combined with the functionality being provided using the power options to support the Green ICT requirements. This functionality has been included in the configuration settings documented at Annex M.~~

~~3.2.2. Folder Redirection~~

~~Folder redirection will be used to:~~

- ~~Reduce the size of roaming profiles, which will optimise performance during logoff and login, and also reduce the impact on network bandwidth;~~
- ~~Reduce the impact of a profile "re-set" during service desk interventions; and~~
- ~~Allow for the use of multiple profiles, supporting a wide range of environments and transitional arrangements.~~

~~Folder Redirection arrangements are included in the *Storage* component of this document.~~

~~3.3.~~3.4. Multimedia Viewer

The Multimedia Viewer is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
a. The multimedia viewer ~~M~~must be capable of supporting at least one of the endorsed codecs. ~~b. Must comply with *Application Management* as defined in the WofG COE Policy~~ ~~Must have endorsed security settings applied in accordance with the WofG COE Policy~~	a. ~~Agencies should ensure that t~~The multimedia viewer ~~can~~ supports the preferred video~~,~~ and audio ~~and DVD~~ playback codec. ~~Agencies need to ensure that applications/systems do not have hardcoded dependencies which would prevent the multimedia viewer complying with N-1 application management~~

Example configuration for the Multimedia Viewer is as follows:

Product Name	Windows Media Player 12
Version	12.0.760~~10~~.*nnnnn*~~16415~~
Installation details	• Installed as an operating system component. • Default install is compliant with the ~~SOE~~WofG COE policy.

Configuration Settings	• Recommended settings Aas detailed at Annex C and Annex D.

~~3.4.~~3.5. Compression Utility

The Compression Utility is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
a. Agencies should use the Windows Compressed Folders feature, or a product compatible with that utility. ~~Must be compatible with the Zip file format version 6.3 of the standard as outlined by PKware~~ ~~a.~~b. The ~~C~~compression utility~~ies~~ should be configured to ensure that the ZIP~~zip~~ file format is the default format. ~~b. Must comply with *Application Management* as defined in the WofG COE Policy~~ c. ~~Must have endorsed security settings applied in accordance with the WofG COE Policy~~	a. The Windows Compressed Folders feature, or a product compatible with that utility, is used for the compression/decompression of files and folders. ~~a. Unicode file names and content are supported in the version 6.3 of the PKware standard~~ b. Using the ZIP file format as the default format for the compression utility promotes compatibility between agencies using compression utilities. ~~To promote compatibility between agencies where a compression utility is used, it should be configured to use the zip file format as the default~~

Example configuration for the compression utility is as follows:

Product Name	~~7 Zip~~Windows Compressed Folders feature
~~Version~~	~~9.15~~
Installation details	• ~~Install: `msiexec /qb /i 7z915-x64.msi`~~ • Installed as an operating system component.~~Default install is compliant with the SOE policy~~
Configuration Settings	• ~~Set default archive format to be ZIP~~ • ~~Enable shell extensions/context menu~~

~~3.5.~~3.6. PDF Viewer

The PDF Viewer is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
~~a. Must comply with *Application Management* as defined in the WofG COE Policy~~ ~~b.~~a. Must support the Open PDF file format as defined by ISO~~/IEC~~ 32000-1:2008. ~~Must have endorsed security settings applied in accordance with the WofG COE Policy~~	a. The Open PDF file format is supported by the PDF viewer. ~~Agencies need to ensure that applications/systems do not have hardcoded dependencies which would prevent the PDF viewer complying with N-1 application management~~

Example configuration for the PDF Viewer is as follows:

Product Name	Adobe Reader X

Version	10.1.*nnnn*~~1~~
Installation details	• ~~Unpack: adberdr10_en_us_std.exe -nos_ne~~ • ~~Install: msiexec /qb /i acroread.msi~~ • Default install is compliant with the WofG COE policy
~~**Example**~~ **Configuration Settings**	

~~3.6.~~3.7. ~~Internet~~Web Browser

The ~~Internet~~ Web Browser is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
~~a. Must be able to be centrally managed and configured~~ ~~b.~~a. The web browser ~~M~~must not allow end user to install unauthorised add-ins. ~~c. Must comply with *Application Management* as defined in the WofG COE Policy~~ ~~Must have endorsed security settings applied in accordance with the WofG COE Policy~~	a. Users ~~should~~are not ~~be~~ able to configure their browsers by installing unapproved add-ins or toolbars.

Example configuration for the ~~Internet~~Web Browser is as follows:

Product Name	Internet Explorer 10~~8~~
Version	~~8.0.7600.16385~~10.0.9200.*nnnn*
Installation details	• Installed as an operating system component. • Default install is compliant with the SOE policy.
Configuration Settings	Recommended settings ~~A~~as detailed at Annex F and Annex G.

~~3.7.~~3.8. Email Client

The Email Client is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
~~a. Must be able to work offline~~ ~~b. Any offline cache data must be stored in accordance with the security classification of that data.~~ a. The email client must support the POP3, POP3S, IMAP, IMAPS, SMTP and SMTPS protocols. ~~c. Must support MAPI/SPOP/SIMAP protocols~~ b. The email client ~~M~~must support shared calendars and contacts. **c.** The email client must support the use of PKI	~~a. A user must be able to read and draft email while disconnected from the corporate network~~ ~~Offline mail cache must be stored appropriately to ensure it cannot be accessed by unauthorised persons~~ a. All common email protocols, and their secure implementations, are supported by the email client. b. Users are capable of viewing shared calendars and contacts.

Standard	Effect
certificates for signing and encrypting email. d. The email client must support the use of an email protective marking solution. e. Email clients should be configured to view emails in plaintext mode. ~~f. Must have endorsed security settings applied in accordance with the WofG COE Policy~~ ~~Must comply with *Application Management* as defined in the WofG COE Policy~~	c. Emails can be encrypted and signed using PKI certificates. d. Protective markings can be applied to all emails. e. Viewing emails in plaintext mode protects against emails being used as a vector for active content attacks.

Any installed email protective marking solutions must comply with the standards specified under the Email Classification Tool component.

Example configuration for the Email Client is as follows:

Product Name	Microsoft Outlook 2010
Version	14.0.4760.*nnnn*~~1000~~
Installation details	• Available as a standalone product or~~Installed~~ as a component of Microsoft Office Professional Plus 2010. • Default install is compliant with the ~~SOE~~WofG COE policy.
Configuration Settings	Recommended settings ~~A~~as detailed at Annex H.

~~3.8.~~3.9. Office Productivity Suite

The Office Productivity Suite is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
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. ~~a. Must support the Office Open XML format as defined by ECMA 376 1st Edition and/or ISO/IEC 29500:2008 standards~~ b. The Microsoft Office File Validation feature should be installed. ~~a. Must comply with *Application Management* as defined in the WofG COE Policy~~ ~~Must have endorsed security settings applied in accordance with the WofG COE Policy~~	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. b. The correctness of file formats can be validated to prevent malformed files exploiting vulnerabilities in Microsoft Office. ~~a. The intention is to standardise on a file format to facilitate the exchange of information between agencies. This does not preclude the use of other file formats.~~ ~~b. An agency's office suite must have the ability to read and write the endorsed file format.~~ ~~Agencies need to ensure that applications/systems do not have hardcoded dependencies which would prevent the Office Productivity Suite complying with N-1 application management~~

Example configuration for the Office Productivity Suite is as follows:

Product Selection	Microsoft Office Professional Plus 2010
Version	14.0.4760.*nnnn*~~1000~~
Installation details	• Default install is compliant with the ~~SOE~~ WofG COE ~~p~~Policy.
Minimum Required Components	• Microsoft Word (All) • Microsoft Excel (All) • Microsoft Outlook (All except Outlook templates) • Microsoft PowerPoint (All except the Organisational Chart add-in) • Visio Viewer (All) • Shared Components (All except non-English proofing tools and web themes) • Office Tools (All except Hosted Web Sites)
Configuration Settings	Recommended settings ~~A~~as detailed at Annex I and Annex J.

~~3.9.~~3.10. VPN Client

The VPN Client is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
a. The VPN client must meet the minimum cryptographic assurance requirements of the *Australian Government Information Security Manual*. ~~a. All requirements for encryption must be in accordance with the Cryptography Section in the ISM Controls Manual~~ ~~b.~~a. The VPN client must use ~~Two~~multi-factor authentication ~~should be used~~ where possible.	a. The VPN client provides sufficient assurance in the protection of sensitive or classified information when in transit. b. Multi-factor authentication provides additional protection against malicious code capturing usernames and passwords. ~~Two factor authentication should be seen as essential for users connecting from a third party network~~

The VPN Client is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *VPN Client* standards as described in this document.

~~3.10.~~3.11. Anti-Virus Client

The Anti-Virus Client is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
~~a. Must support automated deployment~~ ~~b. Must not rely only on pattern based detection methods~~ ~~c.~~a. The antivirus client ~~M~~must prevent end users stopping the service ~~d. The Antivirus solution can be resident in a~~	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

Standard	Effect
~~subsystem such as a hypervisor~~ ~~e. Must support centralised administration, signature/engine updates/reporting~~ b. The antivirus client must automatically and transparently report scanning results. ~~f. Must NOT ask the users permission to report scanning results or install updates~~ c. The antivirus client must be configured to provide the maximum level of protection afforded by the selected product. ~~Must support *Logging* as defined in the WofG COE Policy~~	antivirus client is applied. ~~a. The client must be able to be installed after the deployment of the base image~~ ~~b. Pattern based detection only provides protection on known viruses and does not counter the threat from zero day attacks~~ ~~Where the client is virtualised the Antivirus solution may be installed at the hypervisor level for ease of management~~

The Anti-Virus Client is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *Anti-Virus Client* standards as described in this document.

~~3.11.~~3.12. Firewall Client

The Firewall Client is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
~~a. Must be capable of preventing unauthorised inbound and outbound connections~~ ~~b. Must be supported by central management and configuration~~ a. The firewall client ~~M~~must prevent end users stopping the service. b. The firewall client must be capable of preventing unauthorised inbound and outbound connections at the application layer. c. The ~~F~~firewall client must be able to change its configuration automatically based on location. ~~d. Must support *Logging* as defined in the WofG COE Policy~~ ~~e.~~d. ~~Firewalls should be able to manage network connections from the application level~~	~~a. Refer to the Standard Operating Environments Section in the ISM in the Controls Manual - Installation of software based firewalls limiting inbound and outbound network connections~~ a. Users are unable to disable or bypass the firewall. ~~b. If the firewall solution incorporated into the operating system meets the required standards it should be used. This will reduce complexity and costs and will be updated as part of the operating system~~ b. ~~-~~Network connections ~~should be~~are able to be managed from the application level rather than only filtering on 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.

Example configuration for the Firewall is as follows:

Product Selection	Windows Firewall
Version	6.1.*nnnn*~~7600~~

Installation details	• Installed as an operating system component • Default install is compliant with the WofG COE~~SOE~~ policy
Configuration Settings	Recommended settings ~~A~~as detailed at Annex L

The Firewall Client is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *Firewall Client* standards as described in this document.

3.13. Host-based Intrusion Prevention Client

The Host-based Intrusion Prevention Client is an optional SOE component, but when installed must comply with the following standards:

Standard	**Effect**
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.

The Host-based Intrusion Prevention Client is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *Host-based Intrusion Prevention Client* standards as described in the document.

3.14. Application Whitelisting Client

The Application Whitelisting Client is a *mandatory* SOE component that must comply with the following standards:

Standard	**Effect**
a. The application whitelisting client must prevent users from stopping the service. b. The application whitelisting client uses 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.

Example configuration for the Application Whitelisting Client is as follows:

Product Selection	AppLocker
Version	6.1.*nnnn*
Installation details	• Installed as an operating system component.

	• Default install is compliant with the WofG COE policy.
Configuration Settings	

The Application Whitelisting Client is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *Application Whitelisting Client* standards as described in the document.

~~3.12.~~3.15. Desktop Management Client~~(s)~~

The Desktop Management Client is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
~~a. Must support automated deployment~~ ~~b.~~a. The desktop management client ~~M~~must support remote desktop connectivity for support staff. ~~c.~~b. The desktop management client ~~M~~must support notification of active remote desktop sessions. ~~d.~~c. Must have the ability to collect asset/configuration information ~~e.~~d. ~~Must support *Logging* as defined in the WofG COE Policy~~	a. Support staff are able to remotely troubleshoot and rectify issues with workstation operating systems. ~~a. The client must be able to be installed after the deployment of the base image~~ 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. ~~Unless there is a legal reason, users should be notified of when their desktop session is being accessed by a third party~~

The Desktop Management Client~~, or clients,~~ is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *Desktop Management Client* standards as described in this document.

~~3.13.~~3.16. ~~Message~~Email Classification Tool

The ~~Message~~Email Classification Tool is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
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.

The ~~Message~~Email Classification Tool is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *~~Message~~Email Classification Tool* standards as described in this document.

Installation of an Email Classification Tool addresses the requirements for an email protective marking solution as detailed in standard 'd' of the Email Client component.

~~3.14.~~3.17. Endpoint ~~(USB)~~ Device Control Client~~Agent~~

The Endpoint ~~(USB)~~ Device Control Client~~Agent~~ is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
a. The endpoint device control client must prevent users from stopping the service. ~~a. Must support automated deployment~~ ~~b. Must support central configuration~~ ~~c.~~b. The endpoint device control client ~~M~~must support the disabling of external ports such as USB, eSata, ~~or~~ Firewire, ExpressCard and Thunderbolt to selected user groups. ~~d.~~c. The endpoint device control client ~~M~~must support the disabling of optical drives for both read and write. ~~e.~~d. The endpoint device control client ~~M~~must support the prevention of unauthorised installation of ~~USB~~ devices such as scanners, smartphones, ~~and~~ cameras and mass storage devices such as thumb drives and external hard drives. ~~f. Must support the prevention (and reporting) of the installation of unauthorised USB mass storage devices such as USB thumb drives~~ ~~g. Must be able to record all activity in audit logs which cannot be modified~~ ~~Must support *Logging* as defined in the WofG COE Policy~~	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 are prevented from working with operating systems. ~~a. The client must be able to be installed after the deployment of the base image~~

The Endpoint ~~(USB)~~ Device Control Client~~Agent, or agents,~~ is an *Agency Core Service*, and therefore product selection, installation and configuration remain the responsibility of the agency concerned. The product installed is to be compliant with both the *Common Software Installation Principles* and the *Endpoint ~~(USB)~~ Device Control Client~~Agent~~* standards as described in this document.

~~3.15.~~3.18. Encryption Client

The Encryption Client~~software~~ is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
a. The encryption client must meet the minimum cryptographic assurance requirements of the *Australian Government Information Security Manual*. ~~All requirements for encryption must be in accordance with the Cryptographic Section in the ISM Controls Manual~~	a. The encryption client provides sufficient assurance in the protection of sensitive or classified information when at rest. ~~Where desktop/laptop encryption is required the preferred solution must support at a minimum this level of encryption~~

Example configuration for Encryption is as follows:

Product Selection	Bitlocker
Version	6.1.*nnnn*~~7600~~
Installation details	• Installed as an operating system component • Default install is compliant with the ~~SOE~~WofG COE policy
Configuration Settings	Recommended settings as detailed at Annex E~~As per agency security policies~~

~~3.16.~~3.19. Codec~~s~~ Pack

The Codec~~s~~ Pack ~~are~~is an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect
a. The codec pack ~~M~~must support a codec capable of video playback as defined by the MPEG-4 part 2 standard. b. The codec pack ~~M~~must support a codec capable of audio playback as defined by the MPEG-1 or MPEG-2 Audio Layer 3 standard. ~~On systems with an optical drive, must support a codec capable of DVD playback~~	a. When developing new applications or upgrading legacy applications ~~agencies should use the preferred~~ endorsed codecs are used to promote interoperability. b. Additional codecs may be installed as required

Example configuration for Codecs is as follows:

Product Selection	Windows 7 Codecs
Version	Various – see tables below
Installation details	• Installed as an operating system component • Default install is compliant with the ~~SOE~~ WofG COE policy
Configuration Settings	NIL

~~3.16.1.~~3.19.1. Audio Codecs

Type	Name	Format	Binary	Version
ACM	Microsoft IMA ADPCM CODEC	0011	imaadp32.acm	6.1.760~~0~~.*nnnnn*~~16385~~
ACM	Microsoft CCITT G.711 A-Law and u-Law CODEC	0007	msg711.acm	6.1.760~~0~~.*nnnnn*~~16385~~
ACM	Microsoft GSM 6.10 Audio CODEC	0031	msgsm32.acm	6.1.760~~0~~.*nnnnn*~~16385~~
ACM	Microsoft ADPCM CODEC	0002	msadp32.acm	6.1.760~~0~~.*nnnnn*~~16385~~
ACM	Fraunhofer IIS MPEG Layer-3 Codec (decode only)	0055	l3codeca.acm	1.9.0.*nnn*~~401~~
ACM	Microsoft PCM Converter	0001		
DMO	WMAudio Decoder DMO	0160, 0161, 0162, 0163	wmadmod.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	WMAPro over S/PDIF DMO	0162	wmadmod.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	WMSpeech Decoder DMO	000A, 000B	wmspdmod.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	MP3 Decoder DMO	0055	mp3dmod.dll	6.1.760~~0~~.*nnnnn*

Type	Name	Format	Binary	Version
				~~16385~~

~~3.16.2.~~3.19.2. Video Codecs

Type	Name	Format	Binary	Version
ICM	Microsoft RLE	MRLE	msrle32.dll	6.1.760~~0~~1.*nnnnn*~~16490~~
ICM	Microsoft Video 1	MSVC	msvidc32.dll	6.1.760~~0~~.*nnnnn*~~16490~~
ICM	Microsoft YUV	UYVY	msyuv.dll	6.1.760~~0~~.*nnnnn*~~16490~~
ICM	Intel IYUV codec	IYUV	iyuv_32.dll	6.1.760~~0~~.*nnnnn*~~16490~~
ICM	Toshiba YUV Codec	Y411	tsbyuv.dll	6.1.760~~0~~.*nnnnn*~~16490~~
ICM	Cinepak Codec by Radius	CVID	iccvid.dll	1.10.0.*nn*~~13~~
ICM	VMnc v2	VMC2		
DMO	Mpeg4s Decoder DMO	MP4S, M4S2, MP4V, XVID, DIVX, DX50	mp4sdecd.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	WMV Screen decoder DMO	MSS1, MSS2	wmvsdecd.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	WMVideo Decoder DMO	WMV1, WMV2, WMV3, WMVA, WVC1, WMVP, WVP2	wmvdecod.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	Mpeg43 Decoder DMO	MP43	mp43decd.dll	6.1.760~~0~~.*nnnnn*~~16385~~
DMO	Mpeg4 Decoder DMO	MPG4, MP42	mpg4decd.dll	6.1.760~~0~~.*nnnnn*~~16385~~

~~3.16.3.~~3.19.3. MPEG/DVD Filters

Type	Name	Binary	Version
Video	ffdshow Video Decoder	ffdshow.ax	1.1.*nnnn*
Video	LAV Video Decoder	LAVVideo.ax	0.33.*n.n*
Video	Microsoft DTV-DVD Video Decoder	msmpeg2vdec.dll	6.1.*nnnn*~~7140~~.*n*~~0~~
Video	CBVA DMO wrapper filter	Cbva.dll	6.1.7601.*nnnn*
Audio	ffdshow Audio Decoder	ffdshow.ax	1.1.*nnnn.n*
Audio	Microsoft DTV-DVD Audio Decoder	msmpeg2adec.dll	6.1.*nnnn.n*~~7140.0~~
Audio	LAV Audio Decoder	LAVAudio.ax	0.33.*n.n*

~~3.17.~~3.20. Application Frameworks

The Application Frameworks are an *optional* SOE component, but when installed must comply with the following standards:

Standard	Effect

Standard	Effect
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. Must be in vendor support~~ ~~b. Must comply with *Application Management* as defined in the WofG COE Policy~~ ~~New systems should not have hard coded dependencies on a framework~~	a. Only applications that use an N-1 application framework are deployed on systems. b. Legacy applications that require an application framework outside N-1 have the framework deployed as part of the application and not as part of the operating system. ~~a. Agencies should only support N-1 in their environment. The principle of N-1 is to reduce the complexity and the support requirement for the environment~~ ~~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 SOE~~ ~~New systems or applications should only have a requirement for an N-1 framework. As part of the implementation, maintenance of the new system needs to be factored in so the system will continue to work with the future states of N-1 in the environment~~

Example configuration for the Application Frameworks is as follows:

Product Selection	Version	Installation details
.Net Framework (N)	4.*n*~~0~~	Installed as an operating system component~~dotNetFx40_Full_x86_x64.exe /q /norestart~~
.Net Framework (N-1)	3.*n*~~5 SP1~~	Installed as an operating system component
Java Runtime Environment (N)	Version 7 Update *nn*~~JRE1.6.0_23~~	jre-~~6~~7u*nn*~~23~~-windows-i586~~-s~~.exe /s IEXPLORER=1
Java Runtime Environment (N-1)	Version 6 Update *nn*~~JRE1.5.0_22~~	jre-~~1_5_0_05~~6u*nn*-windows-i586~~-p~~.exe /s /v"/qn IEXPLORER=1 REBOOT=Suppress"
Adobe Flash	~~10.1.82.76~~11.*n.n.nn.nn*	install_flash_player_ax_x64.exe -install
Adobe Shockwave	11.*n.n.nnn*~~5.1.601~~	~~sw_lic_full_installer.exe~~ Shockwave_Installer_Slim.sit /S
Silverlight Runtime	4.0.*nnnn.n*~~50524.0~~	silverlight.exe /q
Microsoft Visual C++ (N)	x64 10.0.*nnnnn* x86 10.0.*nnnnn*	Installed as an operating system component.
Microsoft Visual C++ (N-1)	x64 9.0.*nnnnn.nnnn* x86 9.0.*nnnnn.nnnn*	Installed as an operating system component.
Configuration Settings	~~NIL~~ Consistent with standard DSD hardening guidance for the product, Adobe Flash Player should be configured as follows: • Storage tab – Block all sites from storing information on this computer. • Camera and Mic tab – Ask me when a site wants to use the camera or microphone. If this functionality is not required, choose “block all sites from using the camera and microphone”. • Playback tab – Block all sites from using peer-assisted networking. • Advanced tab – Updates configured as desired by agency.	

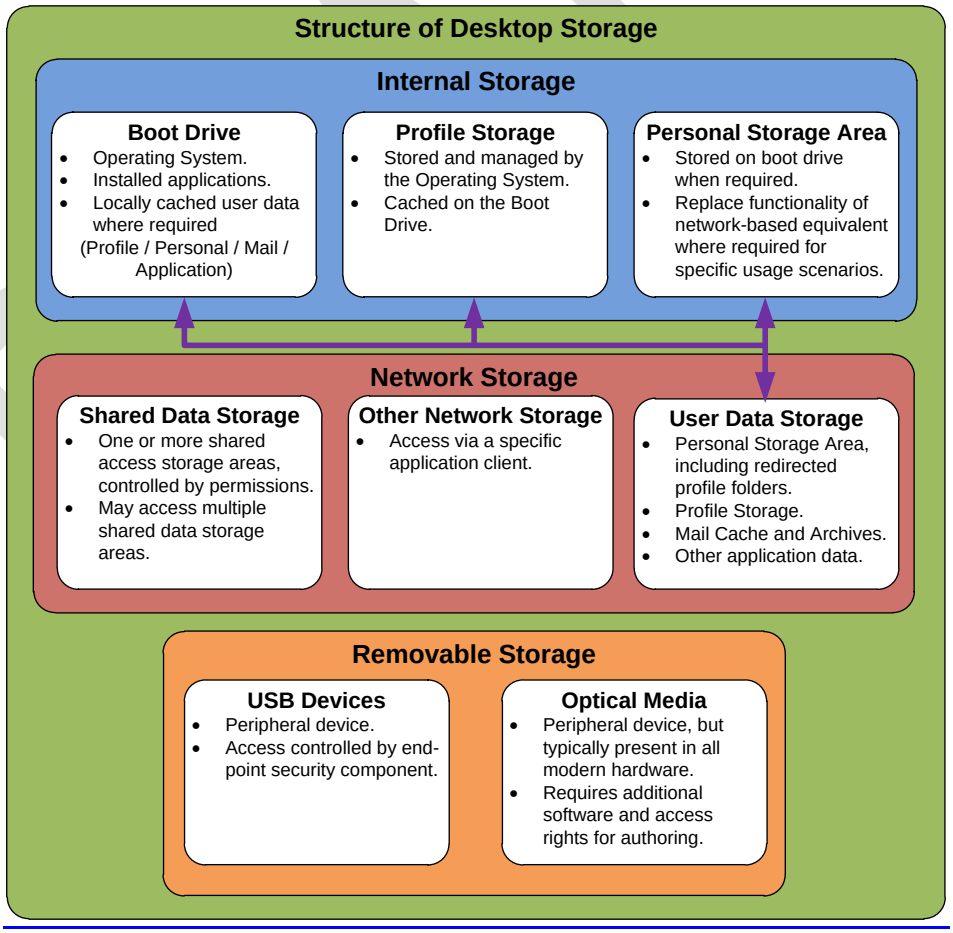
Product Selection	Version	Installation details

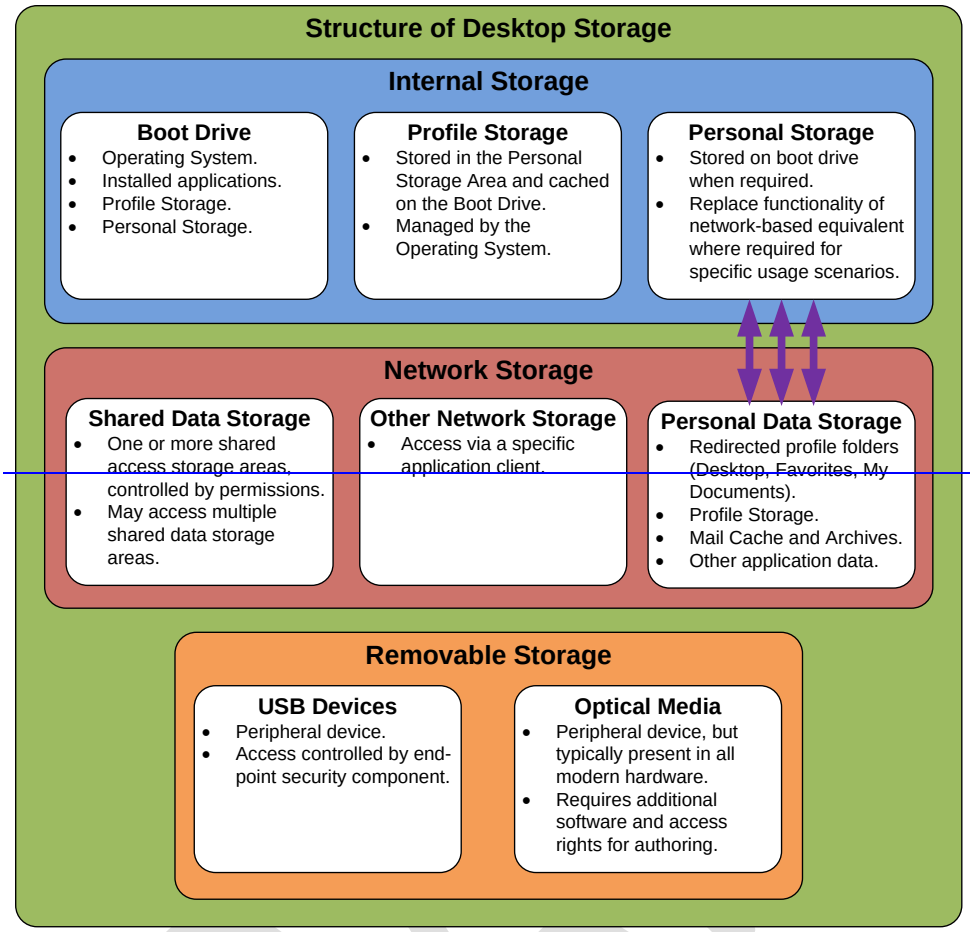
~~3.18.~~3.21. Storage

Storage is a~~n~~ *mandatory~~optional~~* SOE component~~, but when installed~~ that must comply with the following standards:

Standard	Effect
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. Roaming user profiles should be used. ~~a. Data on local hard drives and portable media must be stored in accordance with its security classification~~ ~~Storage of information on local drives is to be avoided~~	a. Sensitive or classification information is either stored on network shares or appropriately encrypted on local workstations. b. Sensitive or classified information on portable devices is appropriately encrypted. ~~a.~~c. Roaming user profiles can be used to provide a consistent experience for users regardless of which workstation they use.~~Data should not be stored on the local systems~~

Storage requirements for the SOE are depicted logically in the following diagram:





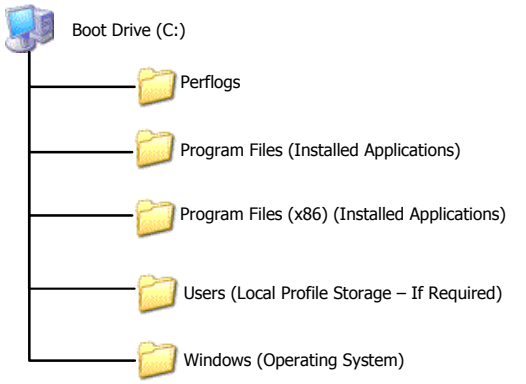
~~As per the ISM, portable workstations that are being used outside of a secure area require encryption for any internal storage. Please refer to the Cryptographic and Working Off-site Sections in the ISM Controls Manual for details. Network storage is a function of the network infrastructure and is out of scope for this document, with the exception of the functionality provided by the personal storage area as outlined below. Requirements for removable storage will depend upon a variety of issues, including the security classification of the data being stored and the agency policies around the use of removable storage, and are therefore also out of scope for this document.~~

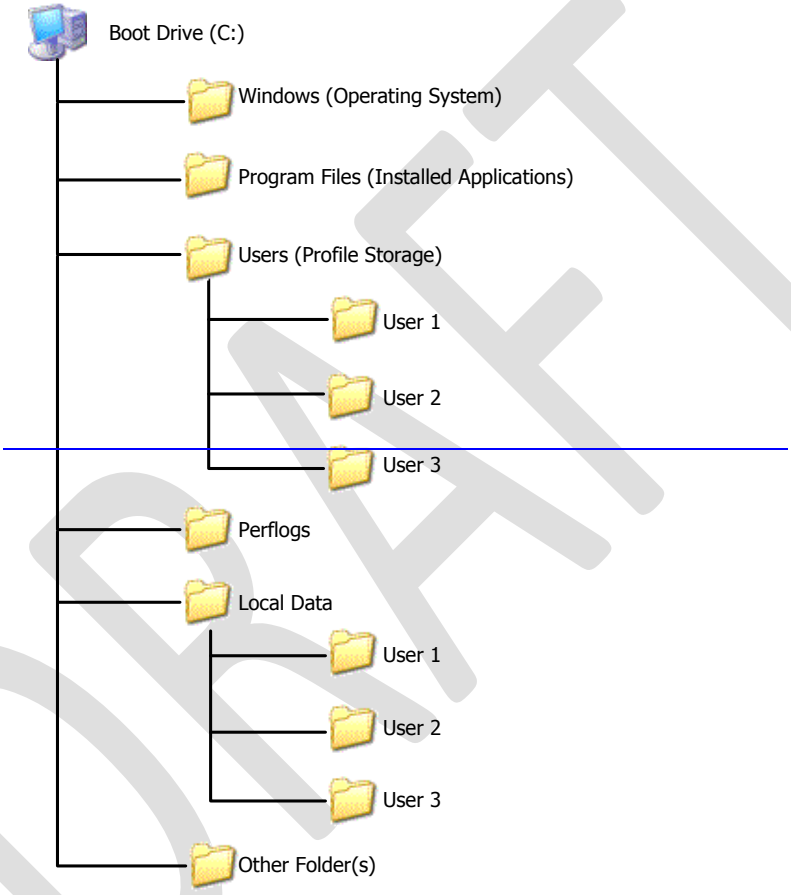
~~3.18.1.~~3.21.1. Boot Drive Configuration

The boot drive will store the following major elements:

- ~~O~~operating system (~~i~~including boot sector and virtual memory),
- ~~i~~installed applications,
- ~~P~~profile storage (where required), and
- ~~P~~personal ~~data~~ storage area (Where required).

With the exception of the personal data storage, these elements will be installed using the default configuration, as depicted in the following diagram:





~~Where required, local personal data storage will be provided by a root level directory on the boot drive named "Local Data". This directory will contain sub-directories, one per user, using the user names as directory names, as per the "Users" directory managed by the operating system.~~

~~3.18.2.~~3.21.2. Profile Storage

Profiles will be stored and managed by the operating system. Active Directory allows for the configuration of a profile for general usage, and a second profile for access via remote desktop technologies. Workstation operating systems beginning with Windows Vista and server operating systems beginning with Windows Server 2008 author version 2 user profiles using the following convention:~~Both of these profiles may be created in two versions, as follows:~~

<User Name>.v2~~: Used by workstation operating systems beginning with Windows Vista or server operating systems beginning with Windows Server 2008.~~

- ~~*<User Name>*: Used by legacy Windows operating systems.~~

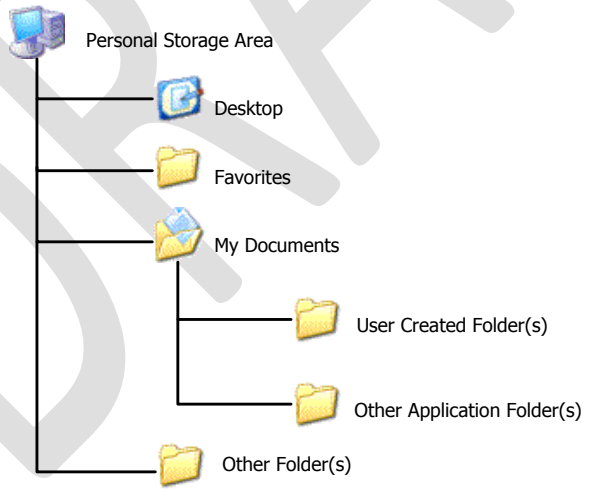
~~Folder redirection will be used to assist in reducing the size of the profile, and to minimise the impacts of having multiple profiles, as described in the next section.~~

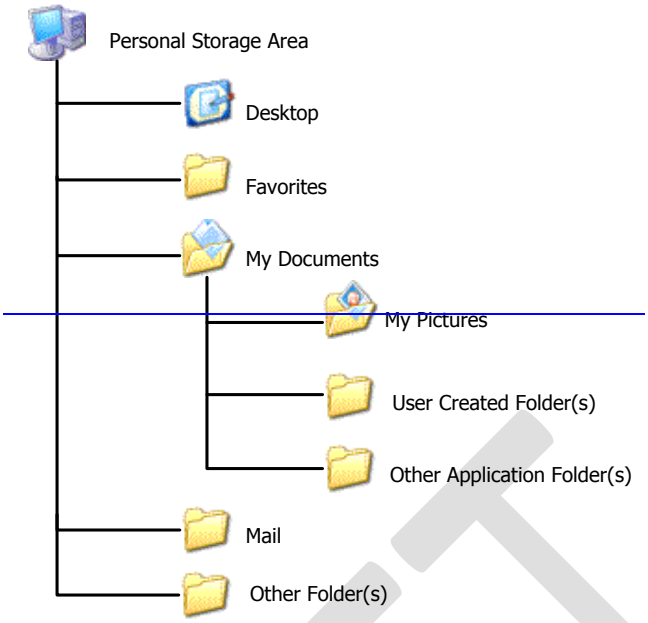
Where users require administrative privileges for their day to day usage, e.g. systems administrators, a separate profile must be created, with restricted access to the Internet and email, for this task. Such profiles should be uniquely named and readily associated with the user. For example, the profiles *joesmith* and *joesmith-admin* could be used to distinguish between standard and privileged profiles of a system administrator.

~~3.18.3.~~3.21.3. Personal Storage Area (Home Drive) Configuration

Each user will require a personal storage area, or home drive, to which they have full read and write access. The personal storage area should~~will normally~~ be maintained on a file server, or other form of ~~n~~Network A~~a~~ttached ~~s~~Storage (NAS) or Storage Area Network (SAN)~~., but may be maintained locally, using suitable encryption, when required for a specific usage scenario. Where the personal storage area is being maintained locally, a solution for replicating the local and network stored versions of the personal storage area may be required.~~

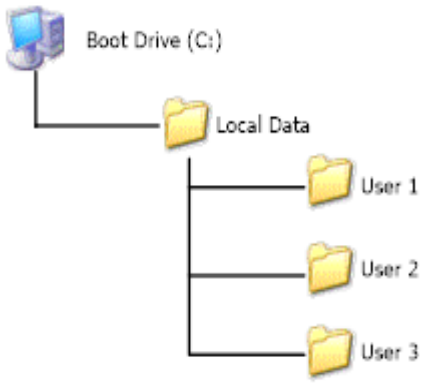
~~The~~Example configuration for the personal storage area ~~will be configured~~ as per the following diagram:





- Folder redirection ~~will~~ should be used to redirect key folders from within the profile into substitute directories within the personal storage area. This may~~will~~ include the "Desktop", "Favorites", and "My Documents" folders, including any content. Folder redirection can be used to:
  - Reduce the size of roaming profiles, which will optimise performance during logoff and login, and also reduce the impact on network bandwidth;
  - Reduce the impact of a profile "re-set" during service desk interventions; and
  - Allow for the use of multiple profiles, supporting a wide range of environments and transitional arrangements.
- ~~A "Mail" folder used to store all electronic mail related content, including cache and archive files.~~
- Other folders may be created as required, and would be used for application data that is not suited to being stored in the "My Documents" folder. Examples include EDRMS cache files, configuration files for enterprise database products like Oracle and DB2, etc.

In specific scenarios a solution for locally storing the personal storage area may be required. This may be achieved by using a root level directory on the boot drive named "Local Data". This directory will contain sub-directories, one per user, using the user name as directory names, as per the "Users" directory managed by the operating system. This is depicted in the following diagram:



~~3.19.~~3.22. Operating System

The Operating System is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
a. The operating system must be procured in accordance with Commonwealth Procurement Rules and in accordance with Whole of Government ICT policies including the ICT Customisation and Bespoke Development Policy.	a. Compliance with the Commonwealth Procurement Rules is maintained.
b. The 64bit (x64) version of the operating system must be used.	b. The enhanced security available in the 64 bit versions of operating systems is utilised.
c. Agencies must adhere to effective patching policies and take into account system importance, patch testing and patch criticality as specified in the ISM.	c. Agencies employ a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities.
d. Patches for the operating system and applications must be able to be deployed remotely without interaction from end users.	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.
e. All applications deployed on the operating system must be approved by the agency.	e. All applications deployed on operating systems are approved by an appropriate Agency authority.
f. Agency approved applications should support automated deployment.	f. Where possible, applications are deployed using an automated process to ensure consistent configuration throughout an environment.
g. Deployed applications must be installed in defined locations only on the operating system.	g. Applications are installed in defined locations, for example, in Program Files, not in a user's home directory.
h. Applications should be centrally	h. Applications are managed in an efficient and

administered and updated. i. Applications should be vendor supported. j. Users must not have write permission to directories that software is executed from. k. Users must not have the ability to manually install unapproved applications, uninstall applications or disable security functionality. l. Multi-factor authentication must be supported. m. Data execution prevention (DEP) must be enabled for essential Windows programs and services, preferably all programs and services with incompatible applications opting-out. n. Where Address Space Layout Randomization (ASLR) is available it must be used. o. Caching of domain credentials should be disabled. p. AutoPlay and AutoRun functionality must be disabled.	consistent manner. i. Vendor support is available for Commercial Off-The-Shelf (COTS) applications. j. Users are prevented from executing arbitrary or malicious software or bypassing application whitelisting. k. User access is limited to the minimum necessary level. l. Multi-factor authentication provides additional protection against malicious code capturing usernames and passwords. m. Data Execution Prevention (DEP) is utilised for all compatible programs and services to assist in mitigating operating system exploits. n. Address Space Layout Randomisation (ASLR) is utilized where available to assist in mitigating operating system exploits. 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.
Operating System Specific Configuration	
q. Structured Exception Overwrite Handling Protection (SEHOP) must be enabled for the operating system. r. LanMan password support must be disabled unless needed for legacy support.	q. SEHOP is utilised for all compatible applications to assist in mitigating operating system exploits. r. The likelihood of passphrase hashes being compromised is reduced.
~~**Standard**~~	~~**Effect**~~
~~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 Development Policy~~ ~~b. Must be capable of supporting the principles outlined in this policy~~ ~~c. Patches for the OS must be able to be deployed remotely without interaction from end users~~ ~~d. Agencies should adhere to effective patching policies that take into account system importance, patch testing and patch severity~~ ~~e. Must have a 64 bit architecture version available~~	~~a. Agencies must first consider an operating system that is a supported COTS product. Any Non COTS solutions must have minimal customisation and there must be an ability to purchase commercial support for the distribution~~ ~~b. Where common operating systems are used, similar build standards, frameworks should be used to allow the sharing of data and packaged applications~~ ~~c. Agencies are encouraged to deploy the 64 bit versions of their preferred operating system~~ ~~d. Operating systems must be able to minimise power consumption by supporting settings such automatic shutdown and sleep mode~~

f. ICT green guidelines need to be taken into consideration in configuration of the operating system g. Power considerations should not impact the deployment of patches h. Must support *Logging* as defined in the WofG COE Policy i. Only applications approved by an appropriate Agency authority are to be deployed j. Deployed applications are to be installed in defined locations only k. Users must not have write permission to directories that software is executed from l. Must have endorsed security settings applied in accordance with the WofG COE Policy m.a. Desktop operating systems and installed software must support IPv6	e. Standard applications are approved as part of the COE and Agencies are responsible for the approval of their own additional business applications. Applications are to be installed in defined locations, for example, in Program Files, not a users home directory f. Users may not have write permission to software executable directories. This prevents users from executing arbitrary or malicious software and bypassing any White listing capability if implemented g.a. IPv6 must be supported by desktop operating systems and installed software

Mandatory security configurations as documented at Annex K as part of the *Security Configuration* SOE component.

Example configuration for the Operating System is as follows:

Product Selection	Microsoft Windows 7 Enterprise with SP1 x64	
Version	6.1.76010	
Minimum Installation Packages	• Microsoft-Windows-Foundation-Package~x86~~6.1.76010.*nnnnn*16385 • Microsoft-Windows-Client-LanguagePack-Package~x86~en-US~6.1.7600.16385 • Microsoft-Windows-LocalPack-AU-Package~x86~~6.1.7600.16385	
Required Features	• MediaPlayback • WindowsMediaPlayer • OpticalMediaDisc • NetFx3 • FaxServicesClientPackage	• Printing-Foundation-Features • MSRDC-Infrastructure • Internet-Explorer-Optional-x86 • SearchEngine-Client-Package
Optional Features	• Printing-Foundation-LPRPortMonitor • WindowsGadgetPlatform • ScanManagementConsole • TabletPCOC • RasRip • RasCMAK • TelnetClient • SimpleTCP • SNMP • WMISnmpProvider • NFS-Administration • ServicesForNFS-ClientOnly • ClientForNFS-Infrastructure • SUA (Services for Unix Applications) • OEMHelpCustomization	• CorporationHelpCustomization • InboxGames • Solitaire • SpiderSolitaire • FreeCell • Minesweeper • PurplePlace • Chess • Shanghai • MSMQ-Container • MSMQ-Server • MSMQ-Triggers • MSMQ-ADIntegration • MSMQ-HTTP • MSMQ-Multicast • MSMQ-DCOMProxy • OpticalMediaDisc • FaxServicesClientPackage
Unused Features	• TelnetServer • Hearts • More Games • Internet Games	• IIS-ServerSideIncludes • IIS-CustomLogging • IIS-BasicAuthentication • IIS-HttpCompressionStatic

	• Internet Checkers • Internet Backgammon • Internet Spades • IIS-WebServerRole • IIS-WebServer • IIS-CommonHttpFeatures • IIS-HttpErrors • IIS-HttpRedirect • IIS-ApplicationDevelopment • IIS-NetFxExtensibility • IIS-HealthAndDiagnostics • IIS-HttpLogging • IIS-LoggingLibraries • IIS-RequestMonitor • IIS-HttpTracing • IIS-Security • IIS-URLAuthorization • IIS-RequestFiltering • IIS-IPSecurity • IIS-Performance • IIS-HttpCompressionDynamic • IIS-WebServerManagementTools • IIS-ManagementScriptingTools • IIS-IIS6ManagementCompatibility • IIS-Metabase • IIS-HostableWebCore • IIS-StaticContent • IIS-DefaultDocument • IIS-DirectoryBrowsing • IIS-WebDAV • IIS-ASPNET • WindowsGadgetPlatform	• IIS-ManagementConsole • IIS-ManagementService • IIS-WMICompatibility • IIS-LegacyScripts • IIS-LegacySnapIn • IIS-FTPServer • IIS-ASP • IIS-CGI • IIS-ISAPIExtensions • IIS-ISAPIFilter • IIS-FTPSvc • IIS-FTPExtensibility • IIS-WindowsAuthentication • IIS-DigestAuthentication • IIS-ClientCertificateMappingAuthentication • IIS-IISCertificateMappingAuthentication • IIS-ODBCLogging • WAS-WindowsActivationService • WAS-ProcessModel • WAS-NetFxEnvironment • WAS-ConfigurationAPI • WCF-HTTP-Activation • WCF-NonHTTP-Activation • MediaCenter • Xps-Foundation-Xps-Viewer • Printing-XPSServices-Features • Printing-Foundation-LPDPrintService • Printing-Foundation-LPRPortMonitor • Printing-Foundation-InternetPrinting-Client • Indexing-Service-Package • TIFFIFilter • TFTP • InboxGames • Solitaire • SpiderSolitaire • FreeCell • Minesweeper • PurplePlace • Chess • Shanghai
Configuration Settings	As detailed at Annex K.	

~~3.20.~~3.23. Network

The Network is a *mandatory* SOE component that must comply with the following standards:

Standard	Effect
a. Applications and network interfaces ~~M~~must support the WofG Internet Protocol Version 6 (IPv6) Strategy. b. Support for IPv6 on network interfaces must be disabled until it is ready to be deployed across the network infrastructure. ~~a.~~c. Support for NetBIOS over TCP/IP must be disabled unless required for legacy support.	a. Applications and ~~N~~network ~~i~~interfaces must support IPV6. b. Enabling IPv6 without proper support on the network infrastructure does not expose workstations to unnecessary security risks. ~~a.~~c. Disabling NetBIOS over TCP/IP reduces the security risk posed to workstations.

The configuration for the *Network* SOE component is as follows:

Product Selection	• Client for Microsoft Networks • Internet Protocol Version 6 • Internet Protocol Version 4
Version	6.1.*nnnn*~~7600~~
Installation details	• Installed as an operating system component ~~Default install is compliant with the SOE policy~~
Configuration Settings	Mandatory settings ~~A~~as detailed at Annex K

~~3.21.~~3.24. Hardware

The Hardware is a~~n *optional*~~*mandatory* SOE component~~, but when installed~~ that must comply with the following standards:

Standard	Effect
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. ~~b.~~e. Hardware must support Wake-on-LAN functionality.	a. All desktops ~~need to be~~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 on hardware 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. ~~a.~~e. Workstations can be woken from Sleep mode across the network to facilitate the application of security patches.

~~All hardware will be procured in accordance with the WofG Desktop Hardware panel, which includes the appropriate driver software to suit this SOE~~