



COTS SECURITY GUIDANCE (CSG)

SUMMARY OF *OVERVIEW OF OPERATING SYSTEM SECURITY FEATURES*

CSG-10\S

August 2009



This page intentionally left blank.



Foreword

The *Summary of Secure use of Operating System (CSG-101S)* is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at itsclientservices@cse-cst.gc.ca or call (613) 991-7654.

Effective Date

This publication takes effect on 08/28/2009.

*Carey Frey
Director, IT Security Industry Program*

© Government of Canada, Communications Security Establishment Canada 2009

It is not permissible to make copies or extracts from this publication without the written consent of CSEC.



This page intentionally left blank.



Table of Contents

Foreword.....	i
Effective Date	i
Table of Contents.....	iii
List of Tables	iv
List of Abbreviations and Acronyms.....	1
Annex A -- Summary of Recommendations.....	3
Annex B -- Security Services Vulnerabilities, Threats and Risks	5
Annex C -- Security Features Checklist for Operating Systems	20



List of Tables

Table 1: LINUX Security Services Vulnerabilities,Threats and Risks	5
Table 2: Mac OS Security Services Vulnerabilities,Threats and Risks.....	10
Table 3: WINDOWS Security Services Vulnerabilities,Threats and Risks.....	17
Table 4: Security Recommendations - LINUX.....	20
Table 5: Security Recommendations – Mac OS X	26
Table 6: Security Recommendations - WINDOWS	33



This page intentionally left blank.



List of Abbreviations and Acronyms

ACL	Access Control List
ANSI	American National Standards Institute
BSD	Berkeley Software Distribution
BTMM	Back to My Mac
CSEC	Communications Security Establishment Canada
CSG	COTS Security Guidance
DAC	Discretionary Access Control
DG	Director General
DNS	Domain Name System
DoS	Denial of Service
FTP	File Transfer Protocol
GC	Government of Canada
GID	Group Identification
GSP	Government Security Policy
HFS	Hierarchical File System
HID	Host Intrusion Detection
HTTP(S)	Hypertext Transmission Protocol - Secure
I&A	Identification and Authentication
IIS	Internet Information Service
IP	Internet Protocol
IPP	Internet Printing Protocol
IPSec	Internet Protocol Secure
IT	Information Technology
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LINUX	Unix-like open source operating system
LPD	Line Printer Daemon

*Secure use of Operating System (CSG-101S)*

Mac	Apple Macintosh operating system
MD5	Message Digest Version 5
OS	Operating System
PC	Personal Computer
POP3	Post Office Protocol 3
RARP	Reverse Address Resolution Protocol
RBAC	Role-Based Access Control
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOW	Statement of Work
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
Telnet	Telecommunication Network
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UFS	Unix File System
UID	User Identification
WINDOWS	Microsoft operating system
X.509	IEEE Standard for Digital Certificates



Annex A -- Summary of Recommendations

Mitigation	Policy
Include Desktop OS in security planning and implementation	Include the desktop OS in IT security program and contingency planning
Disable all unnecessary features	The IT department is responsible for the protection and maintenance
Change default passwords	Require that there be no unauthorized access
Allow only the necessary traffic between the device and a minimum set of trusted addresses	Require authentication for all activities
Require that all IT devices be certified before connection to any network	Define acceptable use policy and make users aware through training
Encrypt data communications	Enforce least privileges
Log all activities extensively	Require periodic security audits
Prevent tampering with audit logs	Require security certification before allowing desktop OS on the network
Employ strong user I&A (e.g., two-factor)	Prohibit the unauthorized copying of sensitive documents
Apply least privileges to users	Prohibit unauthorized external access
Apply the latest software updates and security patches	Require extensive logging of all activities on network devices
Establish thorough change management and auditing programs	Require anti-virus and software updating for all networked devices



Secure use of Operating System (CSG-10IS)

Mitigation	Policy
Use SNMPv3 for centralized management	Prohibit unauthorized network sniffing
Protect the devices physically	Require that IT technology be selected for appropriate security
Require that anyone accessing the device be identified and authorized	



Annex B -- Security Services Vulnerabilities, Threats and Risks

Table 1 below identify the vulnerabilities, threats and risks associated with LINUX OS.

Table 1: LINUX Security Services Vulnerabilities,Threats and Risks

Security Services	Vulnerabilities	Threats	Risks
Identification and Authentication	Account/Authentication Configuration using weak encryption and lack of separation between user names and associated passwords	<ul style="list-style-type: none"> Hackers can decrypt the weak encryption to gain access to passwords. Hackers or malicious users can access passwords for user accounts from the file. 	<p>Unauthorized access</p> <p>Loss or disclosure of information</p>
	<p>Lack of hardening of the GRUB/LILO:</p> <ul style="list-style-type: none"> GRUB password same as 'root' password. GRUB stores the password in clear text. 	Hacker exploitation through weak passwords to gain access to workstation and/or Network.	
Authorization	<p>Weak file System Security contributes to:</p> <ul style="list-style-type: none"> Unrestricted access to administration utilities Default SUID and SGID permissions on executable files. compiler packages from desktops not removed for software development 	Hacker exploitation of workstation and/or Network services.	<p>Unauthorized access</p> <p>Loss or disclosure of information;</p> <p>Malware/worm infection</p>



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
	Weak File/Print Security contributed by: <ul style="list-style-type: none"> • WuFTPd and Anonymous File Serving capabilities¹ • Transient and At-Boot File from external devices/desktops IP address • SAMBA Security in network share • SCP and SFTP services running on desktops². 	Hacker exploitation of workstation and/or Network services.	
Access Control	Firewall installation with default/insufficient parameters attributes to overall weakness for compromise to systems confidentiality, Integrity and availability of the workstation and its information assets.	Hacker compromises workstation through weak firewall settings.	Unauthorized access; Loss or disclosure of information; Malware/worm infection
	No restriction on remote 'root' login.	Hacker compromises workstation through remote login.	
	CTRL-ALT-Delete ³ Running with default configuration can expose the desktops to vulnerabilities that circumvent the DAC.	Hacker compromises workstation through known vulnerabilities in default settings.	

1 Only required if the desktop is required to support FTP services

2 Only allow if the desktop is required to provide some type of file transfer capability for the user per business requirement

3 Highly recommended for desktops with limited physical security.



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
	Weak or no password used to Protect Single-user Mode.	Hacker compromises workstation through known vulnerabilities in default settings.	
	Open System Accounts: Accounts used for system services and/or daemon are allowed to login interactively.		
	TCP Wrapper running with default configuration and accessible to all users.	Hacker compromises workstation through known vulnerabilities in default service settings	
	Scheduler Security: <i>Xinetd</i> enabled and can result in threats originating from telnet, rlogin, wu-ftp or tftp.	Hacker compromises workstation through known vulnerabilities in default service settings	
	Weakness in Web Security configuration: <ul style="list-style-type: none"> • Lack of restrictions on <i>cron</i> and <i>at</i> access can be exploited by threat agents to gain unauthorized access • All web modules are installed • Running with default main configuration file • Default Permission on Files in the Document Root 	Hacker compromises workstation through known vulnerabilities in default Web service settings	
Confidentiality	Accounts created that are not password protected (empty) facilitates access to systems operating system.	External threat agents can gain easy access to information and resources through empty passwords on default accounts	Unauthorized access Disclosure or loss of information Malicious code Data leakage Network exploitation to disclose data traversing the



Secure use of Operating System (CSG-101S)

Security Services	Vulnerabilities	Threats	Risks
			network.
	Weak password policy governing user Account Limits and lengthy password age.	External threat agents can use this to use 'brute force' type attacks to break and gain access to system	
	Sendmail Daemon Mode enabled may <i>Sendmail</i> daemon mode enabled may be used to propagate malware and spam.	A hacker may compromise systems security to enable Sendmail Daemon to disclose data or propagate malicious code.	
	Weak DNS Security: <ul style="list-style-type: none"> No Caching restrictions exposing the network space through sniffing type attacks Lack of zoning can expose the entire network segment to network based attacks 	Network exploitation by a hacker sniffing network for vulnerabilities.	
Integrity	Disabling automated updates service increases risk for compromise through OS weaknesses.	Desktops not configured to use automatic updates via 'up2date' service will leave environment vulnerable to unmitigated known security holes, which hackers can exploit to compromise systems.	Unauthorized access; Malfunction or operation errors
Availability	Partitioning	Lack of strict permission on partition off directories is likely to result in DoS type attacks.	Lack of Availability; Malfunction or operation errors Unauthorized access; Unauthorized disclosure
	Lack of hardening of startup services exposes the environment to threats exploiting unwanted services.	Hacker compromises workstation through known vulnerabilities in enabled startup services.	
Accountability	Accounts have empty passwords	External threat agents can gain easy access to information and resources through empty	Unauthorized access



Secure use of Operating System (CSG-101S)

Security Services	Vulnerabilities	Threats	Risks
		passwords on default accounts	
	Default logging results in insufficient information and event audit.	Malicious activity may go undetected for a prolonged period.	
Non-Repudiation	Unnecessary Accounts resident on workstation are prone to compromise through brute force.	Unnecessary user accounts and groups used by threat agents to gain access	Unauthorized access; Loss of sensitive information
	Audit and logging information lacks accurate time	No synchronization of the system clock with your departments trusted time source(s) can result in operational errors and auditing issues	Operational errors; Malfunctioning of the systems



Table 2 below identify the vulnerabilities, threats and risks associated with Mac OS.

Table 2: Mac OS Security Services Vulnerabilities,Threats and Risks

Security Services	Vulnerabilities	Threats	Risks
Identification and Authentication	Password reset using bootable Mac OS X CD media	Unauthorized access through reset password	Unauthorized access; Malware infection; Security Information exposed
	Use of 'guest' accounts to access other users file or install cron jobs	Malware type infection attacks by via cron jobs	
	"Single User Mode (SUM)" circumvents DAC	'root ⁴ ' level access imparted without authentication	
	'Automatically Log In' is enabled on startup	Access to Mac OS X without any I&A challenge response validation	
	Using 'ypcat password' or 'nidump passwd' type exploits in NIS domain	Access to user accounts and password	
	Weak password policy	Facilitates hackers ability to compromise through weak passwords on user accounts	
Authorization	DAC circumvented when Mac OS X is booted in SUM	Unauthorized access to gain 'root' level access	Unauthorized access;
	"root" user enabled	Unauthorized access gained and privileges elevated by threat agents	
	The initial account used to administer the system, as well as any accounts created prior to changing the umask, allows all users read access to the files in their home folders, public, sites and		

4 In Mac OS X terms root-level access implies full access to all system resources and data.



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
	<p>drop folders.</p> <p>Use of remote management⁵ allowed for all users to control Mac OS X using Apple's remote management application. This feature is similar in some way to the screen sharing function but with the added ability to control the Mac.</p>		
Access Control	All default user accounts are administrative accounts	Unauthorized access to information and resources	Unauthorized operation; Misconfiguration leading to unauthorized access; Loss of sensitive information
	Failure to disable root user facilitates extract of sensitive information from a NetInfo directory	Unauthorized access to executables	
	Case-insensitive nature of HFS+ with respect to security resulting from dependencies built into application code		
	Improper Set-UID bit (SUID) or set-GID bit (SGID) on executables	Unauthorized access to executables through group membership	

⁵ Remote management makes use of the popular VNC server to allow users to connect to the Mac and works with other Open Source VNC clients.



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
	<p>Lack of <i>Firmware Password</i> protection results in</p> <ul style="list-style-type: none"> • Ability to use the "C" key to start up from an optical disc. • Ability to use the "N" key to start up from a NetBoot server. • Ability to use the "T" key to start up in Target Disk Mode (on computers that offer this feature). • Ability to start up in Verbose mode by pressing the Command-V key combination during startup. • Ability to start up a system in Single-user mode by pressing the Command-S key combination during startup. • Reset of Parameter RAM (PRAM) by pressing the Command-Option-P-R key combination during startup. • Use the Startup Manager, accessed by pressing the Option key during startup. • Enter commands after starting up in OF, which is done by pressing the Command-Option-O-F key combination during startup. 	<p>Unauthorized access can be gained by the threat agents using the vulnerabilities related to firmware password</p>	



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
	<ul style="list-style-type: none"> Ability to start up in Safe Boot mode by pressing the Shift key during startup. 		
	Default system-wide security setting enforcement.		
	Using default configuration to displays a list of usernames at the console login prompt.		
	Using Password hints to help users recover their forgotten passwords.		
	Displaying restart, sleep and shutdown buttons on the login window No screensaver activation after a short period of inactivity, and/or NO password required to unlock the workstation.	Unauthorized access resulting from social engineering type exploits	Unauthorized access to information and services
Confidentiality	<i>NetInfo</i> filesystem running under default settings	Unauthorized access to any directory information from <i>NetInfo</i> domain Mac	Unauthorized data access;



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
	Users allowed to use of Back to My Mac (BTMM) to connect to their machine from any other Mac Leopard based server over the Internet.	OS X client is bound to.	Unauthorized information disclosure
Integrity	'Target Disk Mode' means DAC can be circumvented on HFS+ volume by booting from device other than default boot device	Allow root-level access to HFS+ volumes.	Unauthorized information loss and disclosure
	Absence or improperly configured Anti Virus and /or malware prevention software installed on Mac OS desktop	Hackers can use this vulnerability to gain unauthorized access to sensitive information or initiate DoS type attacks	
Availability	Apache server installed on HFS+ volumes can be vulnerable to case-insensitive nature to HFS+	Unauthorized access may result in malfunction through configuration changes	Misconfiguration leading to unavailability
	Using default setting without disabling unused network interfaces such as Airport wireless interface		
	Weakness in the firewall settings leads to compromise the confidentiality, Integrity and availability of the workstation and its information assets.		
	Enabling share and control for remote desktops through VNC.		
	Using Bonjour, formerly known as Rendezvous is Apple's implementation of the ZeroConf protocol. It uses network broadcasts to advertise system services on the local subnet such as printers, iTunes, iChat, SSH and FTP etc.		



Secure use of Operating System (CSG-10IS)

Security Services	Vulnerabilities	Threats	Risks
Accountability	Unattended workstations with disabled systems password and screensaver (keychain) facilitates compromise to systems confidentiality, integrity and/or availability.	Unauthorized access gained through open shells or windows by threat agents using social engineering techniques	Loss of sensitive information
	'out-of-box' setting with "NO" login banner at all points of entry to the system.	Unauthorized operations and access of resources	
	Systems logging and auditing configuration set to default limits capability for adequate logging and incident management.	Host exploitation	Inadequate logging and audit data required to conduct a thorough forensic investigation.
Non-Repudiation	Using 'ypcat password' or 'nidump passwd' type exploits in NIS domain	Access to user accounts and password information	Impermissible as legal and complete evidence during forensic investigation
	'Network time' not a default startup service	Audit and logging information lacks accurate time	
	Using default keychain functionality allows users and applications to store and access authentication details in one place, including store and access private authentication credentials. <i>The password for this keychain is the same as the login password and the keychain is automatically unlocked when a user logs in and is locked again upon logout.</i>		



Table 3 below identify the vulnerabilities, threats and risks associated with WINDOWS OS.

Table 3: WINDOWS Security Services Vulnerabilities,Threats and Risks

Security Services	Vulnerabilities	Threats	Risks
Identification and Authentication	Weak/Non-existent account policies including local accounts as WINDOWS by default has 'blank or null' password on local administrator account	Weak passwords will expose the entire network to threats related to unauthorized access	Malfunctioning; Information loss or disclosure
	Use of LANMAN password encryption	Intruders can access the cached credentials	
	Storing logon credentials in Cache		
Authorization	Lack of review and hardening of minimum privileges required by users and local administrators	More privileges than required will lead to security issues related to compromised user or local administrator accounts	Unauthorized access; Desktop Malfunction
Access Control	Allowing Null Sessions, commonly referred to as 'Red Button' and used by core functions such as Windows Explorer requires anonymous connections to enumerate shares)	Leads to unauthorized access to information and resources such as usernames, groups, administrators, password change dates, account policy, trust relationships and lockout policy	Information disclosure; Desktop Malfunctioning
	Weak / Non-existent Lock out Policies, including remote lockout of administrator accounts	Unauthorized access using "brute force" technique to gain access to information and resources	
	Using default account named 'Administrator'	Default administrator account does not have any lockout enforced thus making them an easy target for 'Brute force' type attacks	
	Default file and network access applied to anonymous users		
	Unrestricted DCOM access	Unauthorized users can change the security setting in the registry keys	



Secure use of Operating System (CSG-101S)

Security Services	Vulnerabilities	Threats	Risks
		for DCOM objects to launch applications/malware	
	Using default settings for 'recycle bin'	Unauthorized users can access deleted files from 'recycle bin'	
Confidentiality	Weak/Non-existent account policies including local accounts as WINDOWS by default has 'blank or null' password on local administrator account	Weak passwords will expose the entire network to threats related to unauthorized access	Malfunctioning; Information loss or disclosure
	Using 'Temp Folder' for terminal services	Common folder used during the terminal services will allow unauthorized disclosure of data files located in shared location	
	Temporary folders are not cleaned on exit	Data files left in temporary folders can be used by hackers to access sensitive information	
Integrity	Lack of Antivirus and Malware protection on all desktops and/or inconsistent use updated definition files for both	Publically known vulnerabilities can be exploited by external threat agents to gain unauthorized access	Information disclosure or loss; Malfunctioning or operating errors
	Windows Messenger active on the desktop	Most anti-virus software don't scan the Windows messenger messages or files thus can be exploited by hackers to launch DoS or malware infection attacks	
	Automatic downloads and updates allowed for media players	Infected codes and other media files downloaded from the internet will result in platform consistency issues	Loss of availability
	Running Internet Explorer with following weak policy settings <ul style="list-style-type: none"> • Disable "Security Zones: use only 	Infected updates can be used by hackers to compromise the desktop OS integrity exposing the sensitive	Unauthorized disclosure; Loss of availability;



Secure use of Operating System (CSG-101S)

Security Services	Vulnerabilities	Threats	Risks
	machine settings” <ul style="list-style-type: none"> • Disable “Security Zones: Do not allow users to change policies” • Disable “Security Zones: Do not allow users to add/delete sites” • Disable “Make proxy settings per-machine” • Disable “Disable Automatic Install of Internet Explorer components “ • Disable “ Disable Periodic Check for Internet Explorer software updates” • Enable “Disable software update shell notifications on program launch” 	information on the network	Malfunction or operation error
Availability	Lack of implementation of service packs Unlimited connections allowed to terminal server	Hackers/disgruntled employee can use this vulnerability to launch DoS attack	Loss of availability
Accountability	Desktop rollout with auditing switched off or with minimum auditing	Unauthorized access attempts will not be visible during the regular system security audits	Unauthorized access to information; Loss of information; Malfunctioning or operating errors
Non-Repudiation	Inadequate security of audit logs	Insufficient logging and audit data can work to threat agents advantage as it minimizes the chances of them being tracked	Impermissible as legal and complete evidence during forensic investigation



Annex C -- Security Features Checklist for Operating Systems

Table 4 below lists, the recommended security features to mitigate the threats associated with LINUX OS.

Table 4: Security Recommendations - LINUX

Security Category	Securing Guidelines	Recommendation Description	Threats Mitigated
Identification and Authentication	Account/Authentication Configuration	<ul style="list-style-type: none"> Choose SHA encryption on passwords. Maintain a shadow file to keep passwords in a separate file from user names. 	Unauthorized access to sensitive security information
	User Account Security	Recommended Password Aging settings in <i>'etc/login.defs'</i> are <ul style="list-style-type: none"> PASS_MAX_DAYS 90 PASS_MIN_DAYS 2 	
	Harden the GRUB/LILO	<ul style="list-style-type: none"> Choose a GRUB password different from <i>'root'</i> password. GRUB stores the password in clear text. Modify <i>'etc/grub.conf'</i> file with SHA password hash value created using <i>'grub-md5-crypt'</i>. 	
Authorization	File System Security	<ul style="list-style-type: none"> Restrict access to administration utilities by removing read, write and execute privileges for users that do not own the files or belong to group the owns the files Remove SUID and SGID permissions from executable files that do not require it Remove compiler packages from desktops not used for software development 	Hackers /Unauthorized users from gaining access to sensitive information; Unauthorized Information Disclosure



Secure use of Operating System (CSG-101S)

Security Category	Securing Guidelines	Recommendation Description	Threats Mitigated
	File/Print Security	<p>Disable WuFTPd tied to User File Transfer and Anonymous File Serving capabilities⁶</p> <p>NFS Client Security for Transient and At-Boot File through configuration setting that include the trusted internal devices/desktops IP address in the <i>'/etc/hosts.allow'</i>.</p> <p>SAMBA Security with respect to the requirement to run <i>'netfs'</i> service on the desktop should be carefully evaluated as it extends the network share to the users of desktop.</p> <p>It is recommended that SCP and SFTP services be disabled on desktops⁷.</p>	
Access Control	Firewall Configuration	<p>Choose <i>'Medium'</i> option for firewall configuration to restrict access to</p> <ul style="list-style-type: none"> • services that utilize ports lower than 1023, • NFS server port (2049), • local X Windows system display for remote X clients, and • X-font server port. 	<p>Hackers /Unauthorized users from gaining access to sensitive information;</p> <p>Unauthorized Information Disclosure</p> <p>Malware infection</p>

6 Only required if the desktop is required to support FTP services

7 Only allow if the desktop is required to provide some type of file transfer capability for the user per business requirement



Secure use of Operating System (CSG-101S)

Security Category	Securing Guidelines	Recommendation Description	Threats Mitigated
	Disallow Remote Root Login	Edit <code>/etc/securetty</code> to restrict <code>root</code> login to the local console.	
	Disable CTRL-ALT-Delete ⁸	Edit <code>/etc/inittab</code> to comment out the following line: <code>'ca:ctrlaltdel:/sbin/shutdown -t3 -r now'</code>	
	Password Protect Single-user Mode	Password Protect Single-user mode is used for system maintenance and hence provides root level access. It is recommended that this mode be password protected at all times.	
	Locking System Accounts	Accounts used for system services and/or daemons should never be allowed to login interactively.	
	Configure access to any enabled services	TCP Wrapper should be configured to <i>deny everything except what is explicitly allowed</i> .	
		<i>Xinetd</i> should be disabled or removed unless telnet, rlogin, wu-ftp or tftp is required to specifically support a business function on the desktop.	
Scheduler Security	<ul style="list-style-type: none"> • Restricting <i>cron</i> and <i>at</i> access through <i>cron.access</i> and <i>at.access</i> file updates. • Ensure that scripts/program being 		

8 Highly recommended for desktops with limited physical security.



Secure use of Operating System (CSG-101S)

Security Category	Securing Guidelines	Recommendation Description	Threats Mitigated
		executed through <i>cron</i> have adequate permissions	
	Web Security	Ensure Only necessary Modules are installed	
		Harden the Main Configuration File	
		Check Permission on Files in the Document Root	
		Encrypt Sensitive Traffic using HTTPS	
Confidentiality	Verify no accounts have empty passwords	Perform search in <i>'/etc/shadow'</i> file for blank second field and all listed accounts should be locked or deleted.	Unauthorized Information Disclosure; Spammers; Network threats
	Miscellaneous Account Limits	Using Pluggable Authentication Module (PAM) enforce the following controls on user accounts <ul style="list-style-type: none"> • System resources limits⁹ (<i>'/etc/security/limits.conf'</i>) • Authorized login origination (<i>'/etc/security/access.conf'</i>) • Regulating login time • (<i>'/etc/security/time.conf'</i>) 	
	Disable Sendmail Daemon Mode	It is recommended that the <i>Sendmail</i> daemon be disabled from all desktops by configuring the <i>'/etc/sysconfig/sendmail'</i> to include	

9 Development desktops will require *soft* limit rather than a *hard* limit



Secure use of Operating System (CSG-101S)

Security Category	Securing Guidelines	Recommendation Description	Threats Mitigated
	DNS Security	DAEMON=no Caching-only Nameserver Zone Hosting Service	
Integrity	Applying Updates and Patches	It is recommended that all desktops be configured to use automatic updates via 'up2date' service. This service should be included in the startup services list.	Desktop Malfunction
Availability	Partitioning	Partition off directories that are most likely to be filled up by an attacker such as /var and /home.	Denial of Service attacks Desktop Misconfiguration;
	Identify Services that should be started	Minimal set at startup should include the following services: <ul style="list-style-type: none"> • keytable • syslog • network • random • crond • anacron • iptables • ntpd Other services should be reviewed for applicability before inclusion in startup list.	Desktop Malfunction leading the unauthorized disclosure



Secure use of Operating System (CSG-101S)

Security Category	Securing Guidelines	Recommendation Description	Threats Mitigated
Accountability	Verify No Accounts Have Empty Passwords	Perform search in <i>'/etc/shadow'</i> file for blank second field and all listed accounts should be locked or deleted.	Hackers
	Logging	<ul style="list-style-type: none"> • Configure <i>'syslogd'</i> service to automatically start on boot • Configure the <i>'syslogd'</i> to send a copy of log messages to remote syslog server • Configure <i>'logrotate'</i> daemon to run following secure setting <ul style="list-style-type: none"> • monthly, • rotate 12, and • compress. • Configure the <i>'logwatch'</i> to send a copy of alerts log messages via Email 	
Non-Repudiation	Purging Unnecessary Accounts	Remove all unnecessary user accounts and groups	Hackers and unauthorized users
	Logging	<ul style="list-style-type: none"> • Configure the <i>'ntpd'</i> to synchronize the system clock with your departments trusted time source(s) 	



Table 5 below lists the recommended security features to mitigate the threats associated with Mac OS X.

Table 5: Security Recommendations – Mac OS X

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
Identification and Authentication	Strengthen user password and account	<p>Develop and strengthen the organisational password policy, adoption the following good practices is recommended:</p> <ul style="list-style-type: none"> • Users cannot reuse the last 3 passwords • Passwords must be at least 8 characters in length • Passwords must contain at least 1 alphabetic and 1 numeric character. • Passwords must be of mixed case and contain at least 1 special character, 1 numeric – <i>this cannot be enforced and should be achieved through user awareness training.</i> • After 3 failed authentication attempts the account is locked out. 	Unauthorized access and disclosure of sensitive information.
	Remove unwanted user accounts	Disable the use of ‘ <i>guest</i> ’ accounts or use ‘Parental Controls’ to lock down ‘ <i>guest</i> ’ account permissions and access.	
Authorization	Disable ‘ <i>root</i> ’ user where possible	The use of “ <i>root</i> ” user is strongly discouraged, and it is recommended that installations should use of administrative users and “ <i>sudo</i> ”.	Unauthorized access
	Harden DAC associated with	Review and change so that only owners	



Secure use of Operating System (CSG-10IS)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
	owners and groups	and groups have read access to the files in their home folders, public, sites and drop folders. This can be achieved using Default Umask and Access Control Lists (ACL)	
	Enforce strong password on remote management	It is strongly recommended that a strong password is set before remote management is enabled; this prevents unauthorised access to the machine.	
Access Control	Harden user accounts	Review default user account settings to remove all administrative access.	Unauthorized access to sensitive information
	Enforce Firmware Password	<p>Enable <i>Firmware Password10</i> for all laptops where strict physical access controls are not possible.</p> <p>Firmware Password protection offers the ability to:</p> <ul style="list-style-type: none"> • Block the ability to use the "C" key to start up from an optical disc. • Block the ability to use the "C" key to start up from an optical disc. • Block the ability to use the "N" key to start up from a NetBoot server. • Block the ability to use the "T" key 	Unauthorized access in environments lacking strict physical access controls

10 Firmware security changes not explicitly endorsed by Apple may result in permanent damage to the computers logic board. Apple has released a graphical tool that sets the firmware password available on the installation disk.



Secure use of Operating System (CSG-10IS)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		<p>to start up in Target Disk Mode (on computers that offer this feature).</p> <ul style="list-style-type: none"> • Block the ability to start up in Verbose mode by pressing the Command-V key combination during startup. • Block the ability to start up a system in Single-user mode by pressing the Command-S key combination during startup. • Block a reset of Parameter RAM (PRAM) by pressing the Command-Option-P-R key combination during startup. • Require the password to use the Startup Manager, accessed by pressing the Option key during startup. • Require the password to enter commands after starting up in OF, which is done by pressing the Command-Option-O-F key combination during startup. • Block the ability to start up in Safe Boot mode by pressing the Shift key during startup. 	
	<p>Strengthen system-wide security settings</p>	<p>It is recommended that following system-wide security settings be used to enforce a secure working environment:</p>	



Secure use of Operating System (CSG-101S)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		<ul style="list-style-type: none"> • Set the requirement of a user having to enter a password to wake the computer from sleep/hibernation mode or to unlock the screen saver. • Disable automatic login by presenting a logon screen. • Require the administrator password to unlock any of the System Preferences panes. • Log the user out after being inactive for 15 minutes of inactivity. • Make use of secure virtual memory, which stops any information in memory from being read. • Disable the remote control function of the system which could otherwise be controlled via infrared. • If you need to remotely connect to your Mac, enable SSH and use the SSH command in the terminal to connect. 	
	Login Display lockdown and password hints	Disable displays a list of usernames at the console login prompt.	
		Disable Password hints across system-wide.	
		Disable restart, sleep and shutdown buttons on the login window.	
Enforce inactivity password	Enforce screensaver activation after 15 minutes of inactivity, and enforce		



Secure use of Operating System (CSG-101S)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		required password to unlock the workstation.	
Confidentiality	Use proper data encryption	Enable data encryption using File Vault and Disk utility per user basis as required to support business role.	Unauthorized data access or modifications
	Disable BTMM	Disable the use of BTMM to connect to their machine from any other Mac Leopard based server over the Internet (TCP port 443 and UDP port 4500).	
	File System and Sharing Security	<ul style="list-style-type: none"> If you do not need to share your Public folder, turn off file sharing altogether. If you need file sharing, be sure that your administrative password is difficult to crack, and Whenever possible, avoid setting file permissions to allow universal write access to folders. 	
Integrity	Up-to-date antivirus and malware protection	Ensure that OS is running latest Anti Virus and Malware detection software. <ul style="list-style-type: none"> Ensure that you set up a scheduled Anti Virus update and scan a minimum of once a week. 	Malfunctioning or Operation errors Viruses and Malicious Code Hackers Unauthorized Access
	Secure install partition	Adopt use of UFS volume for all installs of Mac OS X	
	OS Patching	Leave Software Update enabled and (optional) configure it to update daily instead of weekly.	
	Enable and configure Firewalls	OS X includes two firewalls: <ul style="list-style-type: none"> IPFW-packet-filtering firewall, and 	



Secure use of Operating System (CSG-101S)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		<ul style="list-style-type: none"> Socket Filter Firewall-Application Firewall. <p>Note: ipfw disabled by default.</p>	
Availability	Disable Bluetooth	As a hardening step, disable Bluetooth if it is not required as it adds to the overall security of the system.	Unauthorized access by hackers or unauthorized users
	Harden Firewall access	Enable OS firewall.	
	Remote Control lockdown	ONLY allow sharing and controlling remote desktops through VNC on per user basis as required.	
	Lockdown Bonjour	Lockdown Bonjour or reduce the data being broadcast to discourage hackers.	
Accountability	Limit Administrator Logon	In the environment where there are more than one administrator on a system. The administrative users should be restricted from logging into the system from network services using their administrative accounts. This reduces the risk of authentication credentials being compromised.	Unauthorized access; External attacks such as DoS or Brute Force
	Login Banner	Enforce display of a login banner at all points of entry to the system, usually, login prompts on the desktop, shell logins and other application access prompts. Consult your organization's legal team for an appropriate login banner language.	
	Enhance logging and auditing	Enhance default ' <i>Logging and Auditing</i> ' setting to include the following:	



Secure use of Operating System (CSG-101S)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		<ul style="list-style-type: none"> • Authentication errors; • Remote authentication error; and • Process accounting <p>Ensure <i>syslog</i> service for storage of log information on a secure remote log server.</p>	
Non-Repudiation	Improve Logging security	Enhance the security of the “login” keychain by changing its password to something other than the login password. This ensures that the keychain has to be explicitly unlocked before any items can be accessed and also prevents keychain items from being accessed if the login credentials are compromised.	Unauthorized access



Table 6 below lists the recommended security features to mitigate the threats associated with WINDOWS OS.

Table 6: Security Recommendations - WINDOWS

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
Identification and Authentication	Strengthen password security	<p>Adopt and implement strong password policy including the LOCAL accounts on desktops/laptops. Some suggestions for inclusion in the password policy are 11:</p> <ul style="list-style-type: none"> • Maximum Password Age=Expires in 90 Days • Minimum Password Age = Allow Changes In 5 days • Minimum Password Length = At Least 8 Characters (14 for Administrators) <p>Password Uniqueness = Remember 13 passwords</p>	Malfunctioning; Information loss or disclosure
	Strengthen encryption of passwords	Disable the use of LANMAN password encryption to improve the strength of password hashes.	Malfunctioning; Information loss or disclosure
	Rename administrator account	Rename local account named 'Administrator' to enhance the security posture of the desktop environment	
	Disable caching of logon credentials	Restrict the stored logon credentials to two or less	
Authorization	Harden permissions on all user accounts	Ensure that all administration tasks operate at the minimum necessary privilege level	Unauthorized access to information

11 Password management should follow the departmental / agency security policy or guideline.



Secure use of Operating System (CSG-101S)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		Restrict accounts receiving the right 'Act as Part of the Operating System'.	
Access Control	Disable Anonymous access	"Restrict Anonymous" should be enabled to prevent users from enumerating information related to network	Information disclosure; Malfunctioning or operating errors
	Enable User Lockout	Implement a strict Lock out policy that includes the following elements ¹² . <ul style="list-style-type: none"> • Enable – Account Lockout threshold to "5" • Enable – Account Lockout Duration to "30 minutes"; and • Disable Rest Account Lockout Threshold after 	Information disclosure; Malfunctioning or operating errors
	Restrict access to %SystemRoot%	Implement a strict ACL control on %SystemRoot% that is in line with minimum privileges required for applications to function efficiently	
	Remove "Everyone" from any default file share permissions		
	Restrict DCOM access permissions	<ul style="list-style-type: none"> • Limit the security setting changes in the registry keys for DCOM objects to administrators • Remove registry value for DCOM RunAs Value 	
	Secure 'Recycle Bin'	It is recommended that the 'Recycle Bin' be configured to "remove files immediately when deleted".	
Confidentiality	Strengthen user account policies	Strong password on local administrator account	Malfunctioning;

¹² System owners and administrators need to ensure compliance of lockout policy with organizations security policy.



Secure use of Operating System (CSG-10IS)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
	Disable 'Temp Folder' settings	Setting the 'Do not use temp folders per session' will mitigate the unauthorized disclosure of data files due to common folder during terminal session	Information loss or disclosure
Integrity	Up-to-Date Anti Virus and Malware protection	Implement Antivirus and Malware protection on all desktops and use updated definition files for both	Malfunctioning or operating errors
	Disable Windows Messenger on the desktop	<p>It is recommended that Windows Messenger should be disabled</p> <p>If Windows Messenger is required for use internally a strict lockdown to prevent messenger from accessing internet from desktop</p>	Loss of availability
	Disable automatic downloads and updates for media players	Enable the "Prevent Codec Download" setting to mitigate the risks resulting in platform consistency issues	
	Strengthen Internet Explorer Policy Settings	<p>It is recommended that following Internet Explorer settings be used:</p> <ul style="list-style-type: none"> • Enable "Security Zones: use only machine settings" • Enable "Security Zones: Do not allow users to change policies" • Enable "Security Zones: Do not allow users to add/delete sites" • Enable "Make proxy settings per-machine" • Enable "Disable Automatic Install of Internet Explorer components " • Enable " Disable Periodic Check for Internet Explorer software updates" • Disable "Disable software update shell 	



Secure use of Operating System (CSG-10IS)

Security Services	Security Guidelines	Recommended Description	Threats Mitigated
		notifications on program launch”	
Availability	Up-to-date patch management	<ul style="list-style-type: none"> Implement latest service packs to mitigate security issues from known vulnerabilities Automatic archive process for auditing failures 	Unauthorized access; Malfunctioning or operating errors
	Restrict terminal server connection	Implement ONE terminal server session limit	Loss of availability
Accountability	Enhance auditing	<p>Enable auditing with following options:</p> <ul style="list-style-type: none"> Account logon events – both success and failure Logon events Account management Policy change System events Object Access – success and failure <p>Files, folders, and registry keys must be configured in sync with audit policy.</p>	Unauthorized access; Malfunctioning or operating errors
Non-Repudiation	Secure audit and logging data	<ul style="list-style-type: none"> Implement audit logging on all security related success and failure events included. Limit the clearing and editing of the event logs to authorized members of an Auditors group. 	Hackers and other external threat agents
	Define time synchronization settings	Enable Time synchronization with a secure and authorized time source as this is essential for auditing and authentication purposes	