



Overview of Operating Systems Security Features - WINDOWS

Introduction A key advantage of WINDOWS (includes Windows NT, Windows 2000, Windows XP, and Windows Vista) desktop operating system (OS) is its industry wide support and availability of 3rd party solutions, but this can also present security risks. A WINDOWS desktop that is part of the GC network environment may be compromised by malicious software (malware) or other threats spread through GC networks. Unsecure installation of WINDOWS desktop OS could either expose stored GC information to unauthorized personnel or make critical information unavailable. For these reasons, departments should ensure that WINDOWS desktop OS is configured and used securely.

Life Cycle Security should be addressed in each phase of an OS's life cycle: evaluation, configuration, deployment, management and decommissioning.

Working Environments WINDOWS OS require different security controls depending on what they will be used for. Deployment environments range from Dedicated Production GC office desktops (most secure) to development GC Office desktops (moderately secure) to mobile desktops (least secure) such as receptions, conference rooms, and printing areas.

Basic Security Recommendations

Identification and Authentication – Rename the local Administrator account on desktops and strengthen password security according to departmental password policy.

Authorization– Restrict permissions on all users accounts. Consider implementing minimum necessary privilege level for all accounts.

Access Control – Disable Anonymous access, enable user lockout, remove “everyone” from any default file share permissions.

Confidentiality – Consider strengthening user account policies with Strong password and disable “Temp Folder” settings.

Integrity – Ensure anti virus and malware protection is updated regularly, disable Windows Messenger, disable automatic downloads, and strengthen the Internet Explorer policy.

Availability – Use up-to-date patch management and restrict terminal server connectivity to a single user at a time.

Accountability and Non-Repudiation – Enhance auditing to include success and failures, policy changes, system and logon events, secure audit and logging data, and enable time synchronization with a secure authorized time source.

Security Profile	Working Environment
Least Dangerous (Most Secure)	GC Production Desktops
Moderately Dangerous (Moderately Secure)	GC Development Desktops
More Dangerous (Less Secure)	Shared Desktops
Most Dangerous (Least Secure)	Mobile Desktops