

Windows Best Security Practices v.1.0 6/2008 jf

Server/Workstation/Laptop

1. Install the approved Base level security settings on the system. The policy does the following:
 1. Renames the Administrator account
 2. Creates a dummy account named “Administrator”.
 3. Limits access to the system directly and across the network.
 4. Sets the password complexity requirement.
 5. Sets a default screen saver.
 6. Configures the system for Auto Update
 7. Sets the type of login required.
 8. Enables and sets the login warning screen and text.
 9. Enables auditing of system events.
 10. Sets the size of the event log files.
 11. Vista – Sets the default behavior of the UAC
2. Set a complex password on the renamed Administrator account.
3. Install Anti-Virus software.
 1. Schedule updates
 2. Schedule full scans.
4. Configure the Windows firewall (it’s automatically enabled).
 1. Set for Remote Desktop (if used). Version 6 is allowed past the firewalls.
5. If the system will be part of Active Directory:
 1. Add in the appropriate OUadmins Group to the local Administrators Group.
 2. Use GPO’s to apply tighter security controls.
6. Scan security logs on a Daily/Weekly basis.
7. During image build, use MBSA along with other security tools to check Security Compliance on a sample system. Lock down further as needed.

Laptop

1. Use File Encryption (system and USB drives).
 1. Enable Encrypted File system (EFS) and/or
 2. Use Bitlocker (system must have a data partition to apply) or
 3. Use something like TrueCrypt <http://www.truecrypt.org/>
2. Enable CMOS/BIOS passwords for bootup.
3. Purchase system with Computrace LOJack from Absolute software
 1. This feature assists with either recover of the system, or securely deletes the data from the system at first connection to a network.
 2. This is available through Dell at time of purchase.

USB Drives/Keys

1. Place USB keys in secure locations.
 1. Physically wear the device from a lanyard, or
 2. Attach the key to your key ring.
2. Encrypt the contents of the Key or Drive.
 1. Use something like TrueCrypt.
3. Secure the device with a password.

