

# STEPS FOR SECURING SERVERS

**Make sure all servers are joined to the Domain**

**Make sure Domain Admins and ISServer group are part of the Local Administrators group**

**Rename the Administrator account**

**Give this account a Complex 14 (or longer) Passphrase**

**This Passphrase should be changed every 3 months (90 days)**

**Audit this account and send e-mail when an attempt is made to use this account to logon**

**Create a bogus Administrator account**

**Cut description from renamed Administrator account**

**Paste in description of bogus Administrator account**

**Remove bogus Administrator account from ALL groups**

**Give bogus Administrator account a 14 (or longer) Passphrase**

**Disable the Guest account**

**Remove the Guest account from all groups**

**Disable "Autorun" on the CD ROM**

**Enable "Don't display last logon" (2000 systems is set in registry)  
(2003 is set with GPO)**

**Maintain spreadsheet of all known servers on the network and who is the responsible party for that server.**

**When patches are released, test, and apply to all servers on the network.**

**Server Support should patch all the IS servers**

**Server Support notifies all LAN Admins with servers and:**

**Requires them to report back when this has been done**

**If servers are not patched within the week, notify them that**

**Server Support will patch them.**

**Run scans on all servers after patching is complete.**

**Use two of the three utilities (Retina, Nessus, MBSA)**

**Remediate any vulnerabilities found.**

**\*\* A GPO can manage most of these settings on the Servers OU**

## **ISSUES TO BE CONSIDERED WHEN APPLYING PATCHES**

**Check to make sure McAfee is still running**

**Check to make sure network connections are still in the GUI**

**Check to make sure user accounts that should not be disabled are not disabled**

**Re-run Updates and make sure they all installed**

**Make sure all necessary services for each box are running**

**Make sure Domain Admins are a part of the Local Administrators group.**

**The GPO mentioned above can also control services running on the servers.**