Security Policy recommendations - baseline

Administrator account status	Disabled
Guest Account status	Disabled
Limit local account use of blank password	**Enabled**
Rename administrator account	**<NewName>**
Rename Guest account	Guest
Shutdown system if unable to log security events	Disabled
Digitally encrypt or sign secure channel data (always)	Enable
Digitally encrypt or sign secure channel data (when possible)	Enable
Digitally sign secure channel data (when possible)	Enable
Disable machine account password changes	Disable
Maximum machine account password age	30 days
Require strong session key	Enabled
Do not display last user name	Disabled
Do not require CTRL+ALT+DEL	**Disabled**
Interactive logon: Message for users attempting to log on	**<Have one>**
Number of previous logons to cache	10
Prompt user to change password before expiration	14 days
Require DC authentication to unlock account	Disabled
MS network client: Digitally sign communication (always)	Disabled
MS network client: Digitally sign communication(if server agrees)	Enabled
MS network client: Send unencrypted password to third party	Disabled
MS network server: Amount of idle time required before suspension	15 min
MS network server: Digitally sign communication (always)	Disabled
MS network server: Digitally sign communication(if server agrees)	Disabled

MS network server: Disconnect clients when logon hours expire	Enabled
Network Access: Allow anonymous SID/name translation	**Disabled**
Network Access: Do not allow anonymous enumeration of SAM accts	**Enabled**
Network Access: Do not allow anonymous enumeration of SAM shares	Disabled
Network Access: Do not allow storage of passwords and credentials	Disabled
Network Access: Let Everyone permissions apply to anonymous users	**Disabled**
Network Access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network Access: Do not store LAN Manager hash value	**Enabled**
Network Access: LAN Manager authentication level	**Send NTLMv2** **Refuse LM**
Network Access: LDAP client signing requirements	Negotiate signing
Network Access: Minimum session sec for NTLM SSP -clients	**Require NTLMv2** **Require 128-bit encryption**
Network Access: Minimum session sec for NTLM SSP –servers	**Require NTLMv2** **Require 128-bit encryption**
Recovery Console: Allow automatic administrative logon	Disabled
Recovery Console: Allow floppy copy and access to all drives/folders	Disabled
Shutdown: Allow system to be shutdown without having to logon	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Use FIPS compliant algorithms	Disabled
System objects: Strengthen default permissions on internal system	Enabled
User Account Control: Behavior of the elevation prompt for admins	Prompt for consent for non-Windows binaries
User Account Control: Behavior of the elevation prompt for std users	Prompt for credentials
User Account Control: Detect application installations and prompt	Enabled

User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure in secure locations	Enabled
User Account Control: Run all admins in Admin approval mode	Enabled
User Account Control: Switch to the secure desktop when prompting For elevation	Enabled
User Account Control: Virtualize file and registry write failures to Per-user locations	Enabled