Windows 2008 Server Policy

- **Enforce password history –** 24
- **Maximum Password Age -** 42 days
- **Minimum Password Age –**2 days
- **Minimum password length** - 8 characters
- **Password Complexity -** Enable
- **Store Password using Reversible Encryption for all Users in the Domain -** Disable
- **Account Lockout Duration** - 30 minutes
- **Account Lockout Threshold -** 5 attempts
- **Reset Account Lockout Counter -** 30 minutes
- **Enforce User Logon Restrictions** - Enable
- **Maximum Lifetime for Service Ticket** - 600 minutes
- **Maximum Lifetime for User Ticket** - 8 hours
- **Maximum Lifetime for User Ticket Renewal** - 7 days
- **Maximum Tolerance for Computer Clock Synchronization** - 5 minutes

Windows Audit Policy and Advanced Security Audit Policy (Group Policy)
All Event Log files must be set to 2048KB and must be set to overwrite events as needed.

- **Audit account logon event** - Success, Failure
- **Audit account management** - Success, Failure
- **Audit directory service access** - Failure
- **Audit logon events** - Success, Failure
- **Audit object access** - Success, Failure
- **Audit policy change** - Success, Failure
- **Audit process tracking** - Not configured
- **Audit privilege use** - Success, Failure
- **Audit system events** - Success, Failure
- **Audit Authentication Policy Change** - Success
- **System: System Integrity** - Success, Failure
- **Security System Extension** - Success, Failure
- **Security State Change** - Success, Failure
- **Logoff** - Success, Failure
- **Logon** - Success, Failure
- **Special Logon** - Success, Failure
- **File System** - Success, Failure
- **Registry** - Success, Failure
- **Sensitive Privilege Use** - Success, Failure

Windows Local Security Policy / Group Policy - User Rights Assignment Settings

- **Access Credential Manager as a Trusted Caller** - <no one>

- **Allow Access to this Computer from the Network** - (Restrict the ***Access this computer from the network*** user right to only those users and groups who require access to the computer) Example: Administrators, Domain Administrators
- **Act as Part of the Operating System** - <no one>
- **Add Workstations to Domain –** Administrators
- **Adjust Memory Quotas for a Process** - Administrators, Local Service and Network Service only
- **Allow Log on Locally** - Administrators
- **Allow log on through Remote Desktop Services/Terminal Services** - Remote Desktop Users, Administrators
- **Back up Files and Directories** - Administrators
- **Bypass Traverse Checking** - Restrict the Bypass traverse checking user right to only those users and groups who require access to the computer – for example, Users, network service, local service, Administrators

Windows Local Security Policy / Group Policy - User Rights Assignment Settings
- Contd.

- **Change the System Time** – Administrators, Domain Administrators
- **Change the Time Zone** - Users
- **Create a Page File** - Administrators
- **Create a Token Object** - <no one>
- **Create Global Objects** - Administrators
- **Create Permanent Shared Objects** - <no one>
- **Create Symbolic Links** - Administrators
- **Debug Programs** - <no one>
- **Deny Access to this Computer from the Network** – ANONYMOUS LOGON, Built-in local Administrator account, Local Guest account, All service accounts,
- **Deny Log on as a Batch Job** - <no one>
- **Deny Log on as a Service -** <no one>
- **Deny Log on Locally** - ASPNET account on computers that are configured with the Web Server role
- **Deny log on through Terminal Services/RDP** – Local Guest account, All service accounts
- **Enable Computer and User Accounts to be Trusted for Delegation** - <no one>
- **Force Shutdown from a Remote System** – Administrators
- **Take Ownership of Files or other Objects** - Administrators
- **Generate Security Audits** - Local Service and Network Service only
- **Impersonate a Client after Authentication** – Administrators, Local

Service and Network Service only

- **Increase a Process Working Set** - <no one>
- **Increase Scheduling Priority** - <no one>
- **Load and Unload Device Drivers** – Administrators
- **Lock Pages in Memory** - <no one>
- **Manage Auditing and Security Log** – Local Administrator only
- **Modify an Object Label** - <no one>
- **Modify Firmware Environment Values** - Local Administrator only
- **Perform Volume Maintenance Tasks** - Local Administrator only
- **Profile Single Process** - Local Administrator only
- **Profile System Performance** - Local Administrator only
- **Replace a Process Level Token** - Local Service and Network Service only
- **Restore Files and Directories** - Local Administrator only
- **Shut Down the System** – Administrators
- **Synchronize Directory Service Data** - <no one>

Windows Local Security Policy / Group Policy - Security Options

- **Administrator Account Status** -Disabled
- **Guest Account Status** - Disabled
- **Limit Local Account Use of Blank Passwords to Console Logon Only** - Enabled
- **Rename Administrator Account** – Must be set to something other than Administrator
- **Rename Guest Account** - Must be set to something other than Guest
- **Audit the Access of Global System Objects** -Disabled
- **Audit the use of Backup and Restore Privilege** - Enabled
- **Force Audit Policy Subcategory Settings to Override Audit Policy Category Settings** – Enabled
- **Shut Down System Immediately if Unable to Log Security Audits -** Enabled
- **Prevent Users from Installing Printer Drivers when connecting to Shared Printers –** Enabled
- **Machine Access Restrictions in Security Descriptor Definition Language (SDDL) –** Bespoke for each environment
- **Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) –** Bespoke for each environment
- **Allowed to Format and Eject Removable Media – Administrators**
- **Prevent Users from Installing Printer Drivers -** Enabled
- **Allow Server Operators to Schedule Tasks -** Disabled
- **Digitally Encrypt or Sign Secure Channel Data (Always) -** Enabled
- **Digitally Encrypt or Sign Secure Channel Data (when possible) -** Enabled

- **Disable Machine Account Password Changes -** Disabled
- **Maximum Machine Account Password Age -** 30 days
- **Require Strong (Windows 2000 or later) Session Key -** Enabled
- **Interactive Logon: Display User Information when the Session is Locked -** Enabled
- **interactive logon: Do Not Display Last User Name -** Enabled
- **Interactive logon: Do Not Require CTRL+ALT+DEL -** Disabled
- **Interactive logon: Message Text for Users Attempting to Log On** – For example, ***'By using this computer system you are subject to the 'Computer Systems Policy' of New Net Technologies. The policy is available on the NNT Intranet and should be checked regularly for any updates'***
- **Interactive logon: Message Title for Users Attempting to Log on-** For example ***'Warning – Authorized Users Only – Disconnect now if you are not unauthorized to use this system'***
- **Number of Previous Logons to Cache (in case domain controller is not available)** – 0
- **Interactive Logon: Prompt User to Change Password before Expiration** – 14 days
- **Interactive Logon: Require Domain Controller Authentication to Unlock Workstation** - Enabled
- **Microsoft Network Client: Digitally Sign Communications (always)** – Enabled
- **Microsoft Network Server: Digitally Sign Communications (always)** - Enabled
- **Microsoft Network Client: Digitally Sign Communications (if server agrees)** - Enabled
- **Microsoft Network Server: Digitally Sign Communications (if client agrees)** – Enabled

Windows Local Security Policy / Group Policy - Security Options – Contd.

- **Microsoft network client: Send Unencrypted Password to Connect to Third-party SMB servers** -Disabled
- **Microsoft Network Server: Amount of Idle Time required before Suspending a Session** - 15 minutes
- **Microsoft Network Server: Disconnect clients when Logon Hours Expire** – Enabled
- **Microsoft Network Server: Server SPN target Name Validation Level** – **Accept if Provided by Client** or **Required from Client**
- **Microsoft Network Server: Digitally Sign Communications (always)** – Enabled
- **Network Access: Allow anonymous SID/name translation** – Disabled
- **Network Access: Do not allow anonymous enumeration of SAM**

accounts – Enabled

- **Network Access: Do not allow storage of passwords or credentials for network authentication** – Enabled
- **Network Access: Let Everyone Permissions Apply to Anonymous Users** - Disable
- **Network Access: Named Pipes that can be Accessed Anonymously** – Set to Null, review system functionality
- **Network Access: Remotely Accessible Registry Paths and Sub-paths** - Set to Null, review system functionality
- **Network Access: Shares that can be Accessed Anonymously** - <no one>
- **Network Access: Sharing and Security Model for Local Accounts** – For Network Servers, ***'Classic – local users authenticate as themselves'***. On end-user computers, ***'Guest only – local users authenticate as guest'***
- **Network Security: Allow Local System NULL session fallback –** Disabled
- **Network Security: Allow Local System to use computer identity for NTLM –** Enabled
- **Network Security: Allow PKU2U authentication requests to this computer to use online identities -** Disabled
- **Network Security: Do not store LAN Manager Hash value on Next password Change –** Enabled
- **Network Security: Force Logoff when Logon Hours Expire -** Enabled
- **Network Security: LAN Manager authentication level -** Send NTLMv2 response only\refuse LM & NTLM
- **Network Security: LDAP Client Signing Requirements -** Negotiate Signing
- **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients -** Require NTLMv2 session security
- **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers -** Require NTLMv2 session security
- **Domain controller: LDAP server signing requirements -** Require signing
- **Domain controller: Refuse machine account password changes -** Disabled

Windows Local Security Policy / Group Policy - Security Options – Contd.

- **MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) -** Highest protection, source routing is completely disabled
- **MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes –** Disabled

- **MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended) -** 0
- **System Objects: Require case insensitivity for non-Windows subsystems -** Enabled
- **System Cryptography: Force strong key protection for user keys stored on the computer -** User must enter a password each time they use a key
- **System Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing -** Enable
- **System objects: Default owner for objects created by members of the Administrators group -** Object Creator
- **System objects: Require case insensitivity for non-Windows subsystems -** Enable
- **System objects: Strengthen default permissions of internal system objects (e.g., Symbolic Links) -** Enable
- **System settings: Optional subsystems -** Null value
- **Recovery Console: Allow automatic administrative logon -** Disabled
- **Recovery Console: Allow floppy copy and access to all drives and all folders -** Disabled
- **Domain Controllers Policy- if present in scope - Domain controller: Allow server operators to schedule tasks -** Disabled
- **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies -** Enable
- **User Account Control: Admin Approval Mode for the Built-in Administrator account -** Enable
- **User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop -** Disable
- **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode -** Prompt for consent
- **User Account Control: Behavior of the elevation prompt for standard users -** Prompt for credentials
- **User Account Control: Detect application installations and prompt for elevation -** Enable
- **User Account Control: Only elevate executables that are signed and validated -** Enable
- **User Account Control: Only elevate UIAccess applications that are installed in secure locations -** Enable
- **Enable the User Account Control: Only elevate UIAccess applications that are installed in secure locations policy setting -** Enable
- **User Account Control: Run all administrators in Admin Approval Mode -** Enable
- **User Account Control: Switch to the secure desktop when prompting**

for elevation - Enable

User Account Control: Virtualize file and registry write failures to per-user locations - Enable