Maintenance Checklist

Client: **Date:**

Infrastructure-

Check ✓ **notes:**

- ❑ Network Owners Manual on site
  - Essential documents in notebook (i.e. contact information, backup routine, disclaimer(s), etc.)
  - All relevant software in the notebook
  - LAN diagram showing computer and device locations
  - *Verify that "NO" UserID/Password are noted anywhere in notebook*
- ❑ Internet Service Provider
  - Name of Provider (i.e. AT&T, Time Warner, Embarq, etc.)
  - Make, model, and serial number of modem currently in use
  - Static or Dynamic Public IP address
  - Gateway address
  - DNS servers (verify DNS servers with tools such as http://samspade.org/ and http://www.dnsstuff.com/)
- ❑ Firewall
  - Make, model, and serial number
  - Number of Nodes/Users licensed
  - Device is registered
  - Latest firmware installed
  - Current configuration saved
    - Note custom firewall services (e.g. Terminal Services, Remote Desktop, PC Anywhere, etc.)
    - Note Access Rules in place
  - Correct password configured (i.e., strong password scheme)
  - DHCP disabled if applicable
  - Is DYNDNS being used (i.e., necessary if dynamic public IP)? This should reside on the firewall and not the server(s) or local machine.
  - Note Local Users and verify all others are denied access as expected
  - Allow internet access for all machines where applicable for maintenance and Deny when completed

notes:

- Note if Remote Management (e.g. port :8080) is configured and research further if warranted
- Verify **all** categories are being logged
- Review Log and note or address any irregularities

- ❑ Switches
  - Make, model, and size
  - Number of ports in use
- ❑ Wireless Access Point
  - Make, model, serial number
  - Standard(s) in use (i.e. 802.11a/b/g/n)
  - SSID
  - Channel configured
  - Security/Encryption in use
  - Current configuration saved
  - User Name/Password are noted in CRM software
  - Latest firmware installed
  - Complete a thorough site survey noting any neighboring WLAN's
    - This is a serious security risk and the awareness of any existing WLAN's is desired. (Tools such as: Windows View Available Networks, NetStumbler, and Wifi Sniffer can be used to identify open WAP's, and show channels which may interfere or contend for spectrum)
- ❑ Patch Panel
  - Wiring appearance appropriate
  - Labeled as required (i.e. A, B, etc.)
  - Patch cord lengths appropriate
- ❑ Wall jacks accurately labeled (i.e. corresponds with the port number on patch panel)
- ❑ All devices labeled (i.e. modem, firewall, switch, etc.)
- ❑ Note other networked devices (i.e. x-Ray machine, printer, scanner, camera, digitizing pad, etc.). Networked devices can be discovered using a program such as Angy IP Scanner (understand all IP's used and what is using them)
- ❑ Power cycle all devices to verify all work correctly after a power outage
  - Essential devices powered from a UPS (i.e. modem, firewall, switch, etc.)

Note any other maintenance items performed / abnormalities discovered / recommendations:

Server(s)-

Check ✓

notes:

- ❑ Note version of Anti-Virus/Anti-Spyware software installed, verify such is running in real-time, and is currently up-to-date
  - Configure exclusions (e.g. Specialty software, etc.)
  - Run or print a scan report for the period of time since last maintenance
  - Verify Anti-Virus workstation agent is communicating with host machine (i.e. Online or Offline)
  - Verify scheduled scans are configured appropriately and **before** the daily backup
  - If warranted perform an online third party scan:
    - BitDefender, Panda, Avast, McAfee, Trend Micro, KasperSky, Symantec, WindTrojScan, CA, Nod32, F-Prot, OneCare, ESET
- ❑ Data Backup
  - Note backup software in use (i.e. SBS Backup, NT Backup, Symantec Backup Exec (Veritas), NovaNet-WEB, ViceVersa etc.)
  - Note current amount of data being backed up and data rate (i.e. the rate at which data is saved)
  - Note the size of backup media (i.e. size of tape or external drive, etc.)
  - Verify a backup to alternating workstation(s) configured
  - Review logs and address issues that may be preventing successful backups
- ❑ Reset the browser Security Zones to their Default Level, and the browser Advanced tab to Default Settings (i.e. reset all changed settings). Re-configure browser settings for any specialty applications online applications
- ❑ Install the latest **Microsoft** Updates (i.e. Windows, Office)
  - Note number of updates applied
  - Verify the latest version of Remote Desktop Connection installed
- ❑ Note remote access software installed and in use
  - PC Anywhere
  - Remote Desktop
  - RealVNC
  - LogMeIn

notes:

- CrossLoop
- GoToMyPC
- WebEx
- Other:
  - Recommend workstations be accessed for running applications and the server be accessed only to work on the server…

- ❑ Note currently Scheduled Tasks and determine their appropriateness
- ❑ Review Add/Remove programs, note any problematic software (i.e. software which is a potential security risk)
- ❑ Inspect software which require updates/patches (e.g., Secunia Software Inspector)
- ❑ Review the System Configuration Utility "Startup" items, research vague items
- ❑ Run Microsoft's Malicious Software Removal Tool (i.e. Full Scan). This will be done with the installation of IE7 w/Microsoft Updates
- ❑ Administrator password conforms to suggested "strong password" scheme
- ❑ Screensaver wait time is set accordingly and configured to password protect on resume
- ❑ Add a Description for each of the Client Computers in the Server Management Console
- ❑ Is folder redirection being employed, if not data being placed at risk
- ❑ Verify specific Power Management is turned off (i.e. monitor, Ethernet, USB root hub)
- ❑ Verify fan(s) are working (i.e. CPU, Case, Power Supply, etc.)
- ❑ Ensure server and monitor are powered through at minimum a UPS, ideally a Power Conditioner & UPS
- ❑ Inventory machine (e.g. Aida32), create and save a report
  - Verify the latest program(s) version is installed and are up-to-date (e.g. run Live Update, Quick Time, WinZip, IM, Skype, etc.)
  - Note **illegitimate** software installed (i.e. personal or non enterprise versions, etc.) and recommend its removal if installed by client (e.g. Ad-Aware, Spybot, Belarc, MS Office, etc.)
- ❑ Verify Microsoft's Baseline Security Analyzer (MBSA) is installed, run and review report and address any critical issues, missing patches and updates

notes:

- ❑ Do a regular IP scan (e.g., w/AngryIP) of IP's on your network; verify you can associate all of them to known machines and/or devices. Research unrecognized IP addresses.
- ❑ Review the Event Viewer logs
  - Address error events
  - Clear All Events saving the existing log to a file
- ❑ Verify Diskeeper (if used) is installed or other de-fragmentation software
  - Hard drive is not critically fragmented (previously ran)
  - Appropriately scheduled (e.g. weekends only)
- ❑ Note Hard Drive utilization
- ❑ Verify Disk Quotas are disabled if applicable
- ❑ Review Monitoring and Reporting, configure as required (e.g. send email when system is restarted, etc.)
- ❑ Licensing
  - Note installed licenses
  - Note maximum usage
  - Review Users
  - Review Client Computers
- ❑ Verify UserID/Password are noted in CRM software
- ❑ Note if the latest version of DynDNS Updater is installed if applicable (unnecessary if client has a static IP) verify client is listed in the "Hosts (A) Records" at www.dyndns.org
- ❑ Review the system "hosts" file (C:\Windows\System32\drivers\etc).
- ❑ Verify DNS servers with tools such as http://samspade.org/ and http://www.dnsstuff.com/
- ❑ Exchange? (need a better understanding of this service and its issues)
- ❑ Blackberry? (need a better understanding of this service and its issues)
- ❑ Restart machine(s)

Note any other maintenance items performed / abnormalities discovered / recommendations:

Computer Name: **Description:**

Workstation(s)-

Check ✓ **notes:**

- ❑ Recommend/remind that users "Log Off" workstations at the end of each business day, and "Shut Down" workstations at the end of the week to allow scheduled tasks to run (i.e. virus/malware scans, disk de-fragmentation, etc.)
- ❑ Verify administrator password for local machine is set and conforms to the suggested scheme (i.e. strong password)
- ❑ Reset the browser Security tab Zones to Default Level, and the browser Advanced tab to Default Settings (i.e. reset all changed settings). Re-configure browser settings for online applications (i.e. Centricity, etc.) as required
- ❑ Install the latest Microsoft Updates (i.e. Windows, Office)
  - Note number of updates applied
  - Install the Remote Desktop Connection update (within Software Updates)
- ❑ Install Wireless Client Update on all laptop computers
- ❑ Note version of Anti-Virus/Anti-Spyware software installed, verify it is running in real-time, and is currently up-to-date
  - Configure exclusions (i.e. Specialty software, etc.)
  - Run or print a scan report for the period of time since last maintenance
  - Verify Anti-Virus workstation agent is communicating with host (server) machine
  - Verify scheduled scans configured appropriately
  - If warranted perform an online third party scan:
    - BitDefender, Panda, Avast, McAfee, Trend Micro, KasperSky, Symantec, WindTrojScan, CA, Nod32, F-Prot, ESET
- ❑ Security Center
  - Firewall on
  - Automatic Updates off
  - Virus Protection on
  - Un-check the Security Center Alert for Automatic Updates
- ❑ Install program which monitors and displays the CPU temperature (e.g. Speedfan)
  - Configure to run minimized
  - Configure to run in the Startup of All Users
  - Configure to Use Fahrenheit

- Eliminate dust within machine if warranted

notes:

- ❑ Verify all fan(s) are working (i.e. CPU, Case, and Power Supply)
- ❑ Note remote access software installed and in use
  - PC Anywhere
  - Remote Desktop
  - RealVNC
  - LogMeIn
  - CrossLoop
  - GoToMyPC
  - WebEx
  - Other:
    - Recommend workstations be accessed for running applications and the server be accessed only to work on the server…
- ❑ Inventory machine hardware/software (e.g. Aida32), create and save a report
  - Verify installed programs are up-to-date (e.g. QuickBooks, run Live Update, Quick Time, WinZip, IM, Skype, etc.)
  - Note illegitimate software installed i.e. personal or non enterprise versions, and recommend its removal if installed by client (e.g. Ad-Aware, SpyBot, Belarc, etc.)
- ❑ Note the amount of RAM currently installed and make recommendations where applicable
- ❑ Verify other commonly used software installed (i.e. Java, Adobe Reader, etc.) has latest updates/patches installed Inspect software which require updates/patches (e.g., Secunia Software Inspector)
- ❑ Verify Microsoft's Baseline Security Analyzer (MBSA) is installed, run and review report and address any critical issues, missing patches and updates
- ❑ Note Hard Drive utilization and make recommendations where applicable
- ❑ Run Microsoft's Malicious Software Removal Tool (i.e. Full Scan), installed w/IE7 from Windows Updates.
- ❑ Windows Disk Defragmenter script is scheduled to run off hours once a week
- ❑ Workstations plugged into a power surge protector (minimum). Recommend using UPS's, or Power Conditioners for all machines not only to prevent "Black Outs", but "Brown Outs" or low voltage damage

- ❑ Review startup items and note any needing further examination
- ❑ Review the System Configuration Utility “Startup” items, research vague items
- ❑ Note all currently Scheduled Tasks
- ❑ Schedule task to weekly de-fragment the hard drive(s)
- ❑ Schedule task(s) to logoff user and shutdown workstation if required (optional)
- ❑ Note installed “illegitimate” software (i.e. personal or non enterprise versions, etc.) and recommend its removal if installed by client (e.g. Ad-Aware, SpyBot, Belarc, etc.)
- ❑ Note problematic software being used (i.e. Instant Messaging, Outlook Express, Remote Access, HTTP email, etc.)
- ❑ Review Add/Remove programs and recommend removal of problematic software (i.e. potential security risk)
- ❑ Add a Computer Description to each Windows XP machine
- ❑ Verify UserID/Password are noted in CRM software
- ❑ Verify specialty application software has unique UserID/Passwords recommend such if not in use
- ❑ Verify workstation Screen Saver has “On Resume, Require Password” checked, where applicable. If not configured, recommend it
- ❑ Install Microsoft Office 2007 Compatibility Pack and associated updates if applicable
- ❑ Turn off Run Desktop Cleanup Wizard every 60 days
- ❑ Optimize the desktop for best performance and configure classic start menu (optional)
- ❑ Review the system “hosts” file
- ❑ Note any other devices connected to machine (i.e. peddles, intra-oral cameras, scanners, printers, wired/wireless x-ray sensors, card slots, external drives, plotters, etc.)
- ❑ Restart machine if not ask to do so previously

notes:

Note any other maintenance items performed / abnormalities discovered / recommendations: