General Motors
Dealer Infrastructure Guidelines

2016

v.16.4

Section 1: Guidelines Summary & Notes
Section 2: Dealer IT Guidelines Detail
Section 3: Appendix A

Section 1: Guidelines Summary & Notes

GM has adopted these infrastructure guidelines for the dealership's internal network environment in accordance with Article 5.6 of the Dealer Sales and Service Agreement. These guidelines are designed to ensure a seamless and reliable conduit for GM to dealer data communications.

The infrastructure guidelines are organized as follows:

- **Recommended** – the systems infrastructure components that will deliver performance and security while seeking to maximize the lifecycle of the investment. If you are looking to purchase new systems, please adhere to the specifications outlined in the "recommended" section.

- **Minimum** – the lowest acceptable systems infrastructure for conducting business with GM

The recommended and minimum guidelines apply to PC systems as well. Specific, detailed information appears in each section of the document.

Please Note the Following: Dealerships may choose processor speeds, memory capacities, audio adapters and hard drive capacities which exceed the recommended specifications based on needs and product availability.

General Motors estimates the life cycle of a Desktop PC, Laptop or Tablet PC on average is three (3) years.

For the Techline Service Technician applications (TIS2Web, GDS2, MDI, MDI 2, Tech2Win, Service Information)

Supported	Not Supported
Intel i3 / i5 / i7 processors	ALL Processors below the Intel i series plus AMD, Celeron and Atom processors
Business grade hardware (PC and Access Points)	Consumer grade hardware (PC and Access Points)
**Windows 10 Professional,64 bit	Non branded, built by hand or thin client PCs
Windows 7 Professional 64 bit	Tablets running Android or Mac operating systems
***Internet Explorer (IE) 11 32 bit	Windows XP and Vista Business
	Any Home version Operating System
	Windows 8.x
	Internet Explorer (IE) 10 and below ***see exception below
	All Internet Explorer and Java 64 bit versions
*Refer to Section 2 for details	Apple or Mac tablets, PCs

Techline:

- Requires Local Windows Administrative access for software installation and updates
- Refer to Appendix A (Section 3) for a list of recommended firewall and security exceptions
- Requires one (1) laptop minimum for use with the GDS2 application
- Recommends one (1) laptop for every two (2) technicians
- Recommends one (1) Multiple Diagnostic Tool (MDI / MDI 2) for every Techline PC
- Recommends one (1) battery maintainer for every two (2) Multiple Diagnostic Interface (MDI) tools in use

For questions related to the GM Infrastructure Guidelines, contact GMDIT at 888-337-1010, Prompt 4. For specific Service or Parts department PC questions related to Dealership Infrastructure Guidelines, contact http://gmdesolutions.com at 800-GMTOOLS or Techline at 888-337-1010 prompt 3.

Section 2: Dealer IT Guidelines

DESKTOP PC

Recommended: **Guidelines for purchasing new hardware**	
Processor	Intel Core i3, i5, i7 2nd Generation* or above (See note below)
System Memory (RAM)	**4 GB or more (See note below)
Hard Disk Drive	***1 TB or more (See note below)
CD / DVD Drive	CD/DVD Combo
Serial Port	1 (optional USB convertor)
USB Ports	4 or more
Audio Speaker	Required
Network Adapter	Ethernet based 100/1000Mbps (100/1000BasedT) Optional wireless WAN802.11g
Warranty	3 year onsite
Operating System	Windows 10 Professional, 64 bit
Printer	Networked Laser Printer

***Note 1**: 2nd Generation or above have model numbers of 2000 or greater (example: Intel Core i3-**2100**).
****Note 2**: Windows 7 32 bit supports up to 4GB of memory, but the actual usable address space will be less than 4GB.
*****Note 3**: Drive space increase to accommodate Techline Data Service (TDS) calibration files

The following provides what General Motors considers the minimum requirements to run dealership applications. Do not reference the minimum specification when purchasing a new PC, but rather use it as a comparison for hardware being transitioned from one department to another.

Minimum: **Do Not Reference For New Hardware Purchase**	
Processor	Intel Core i3, i5, i7 1st Generation
System Memory (RAM)	2 GB
Hard Disk Drive	320 GB
CD / DVD Drive	CD / DVD Combo
Serial Port	1
USB Ports	4
Audio Speaker	Required
Network Adapter	Ethernet based 100 Mbps (100BaseT)
Operating System	Windows 7 Professional, 64 bit
Printer	Black and White Laser

GM does not support Windows XP Mode / Windows Virtual PC on Windows 7 Professional.

LAPTOP PC and TABLET PC

Recommended: **Guidelines for purchasing new hardware**	
Processor	Intel Core i3, i5, i7 2nd Generation* or above (See note below)
System Memory (RAM)	**4 GB or more (See note below)
Hard Disk Drive	500 GB or more
CD / DVD Drive	CD/DVD Combo
Serial Port	1 (optional USB convertor)
USB Ports	4 or more
Audio Speaker	Required
Video	1024 x 768 resolution or greater, 32 bit color, 128 MB video memory
Display	15.4 inch
Network Adapter	Ethernet based 100Mbps (100BaseT) Optional wireless WAN802.11g
Warranty	3 year onsite
Operating System	Windows 10 Professional, 64 bit

***Note**: 2nd Generation or above have model numbers of 2000 or greater (example: Intel Core i3-**2321**M).
****Note**: Windows 7 and 10 32 bit supports up to 4GB of memory, but the actual usable address space will be less than 4GB.

Minimum: **Do Not Reference For New Hardware Purchase**	
Processor	Intel Core i3, i5, i7 1st Generation
System Memory (RAM)	2 GB
Hard Disk Drive	320 GB
CD / DVD Drive	CD / DVD Combo
Serial Port	1
USB Ports	4
Audio Speaker	Required
Video	1024 x 768 resolution or greater, 32 bit color, 128 MB video memory
Display	15.4 inch
Network Adapter	Ethernet based 100 Mbps (100BaseT) Wireless 802.11g
Operating System	Windows 7 Professional, 64 bit

- Some GM applications are specifically developed to run on certain tablet devices, such as iPads. When these applications are deployed, GM will communicate which devices those applications are intended to be used.
- Based on the evolving technology in the mobile space, the compatibility of certain programs may be limited to specific tablets and/or mobile device operating system version.

GM Global EPC (Electronic Parts Catalog)

Hardware Requirements Server and PC Standalone

	RECOMMENDED SERVER SPECS	RECOMMENDED PC SPECS
Processor	Intel® Quad Core Xeon or better	Intel® Core™ i5 or better
RAM	16 GB	8 GB
Web Browser	Internet Explorer 11 (Edge browser not supported)	Internet Explorer 11 (Edge browser not supported)
Free Disk Space (DVD Users)	GM US and Canada: 250 GB free disk space	GM US and Canada: 250 GB free disk space
	GM Europe: 200 GB free disk space	GM Europe: 200 GB free disk space
	Holden: 200 GB free disk space	Holden: 200 GB free disk space
	GM de Mexico: 250 GB free disk space	GM de Mexico: 250 GB free disk space
	GM International: 600 GB free disk space	GM International: 600 GB free disk space
	GM South America: 250 GB free disk space	GM South America: 250 GB free disk space
	GM do Brasil: 175 GB free disk space	GM do Brasil: 175 GB free disk space
Operating System	Server 2012 "Standard" and "Enterprise" editions	Windows 7 "Professional" and "Enterprise" editions

***Notes:**

- When selecting a new computer that will be used for the GM Global EPC, we recommend the purchase of hardware with a (minimum) 1TB hard drive. The Free Disk Space requirements above should be referenced when determining if currently owned hardware can support local EPC installation. If the web version of the EPC is used, there is a very minimal amount of free disk space required.
- To ensure proper function of the GM EPC, internet content filters should be updated to allow *.epclink.com.

	MINIMUM SERVER SPECS	MINIMUM PC SPECS
Processor	Intel® Dual Core Xeon or better	Intel® Core2Duo, or better
RAM	4 GB	4 GB
Web Browser	Internet Explorer	Internet Explorer
Free Disk Space (DVD Users)	GM US and Canada: 250 GB free disk space	GM US and Canada: 250 GB free disk space
	GM Europe: 200 GB free disk space	GM Europe: 200 GB free disk space
	Holden: 200 GB free disk space	Holden: 200 GB free disk space
	GM de Mexico: 250 GB free disk space	GM de Mexico: 250 GB free disk space
	GM International: 600 GB free disk space	GM International: 600 GB free disk space
	GM South America: 250 GB free disk space	GM South America: 250 GB free disk space
	GM do Brasil: 175 GB free disk space	GM do Brasil: 175 GB free disk space
Operating System	Server 2008 "Standard" and "Enterprise" editions.	Vista or Windows 7 "Professional" and "Enterprise" editions

***Notes:**

- When selecting a new computer that will be used for the GM Global EPC, we recommend the purchase of hardware with a (minimum) 1TB hard drive. The Free Disk Space requirements above should be referenced when determining if currently owned hardware can support local EPC installation. If the web version of the EPC is used, there is a very minimal amount of free disk space required.
- To ensure proper function of the GM EPC, internet content filters should be updated to allow *.epclink.com.

PC SOFTWARE FOR GLOBALCONNECT APPS

Recommended:	
Word Processing	MS Office Viewer
Spreadsheets	MS Office Viewer
Presentation	MS Office Viewer
Web Browser	Internet Explorer, version IE11 (with current Service Pack) with the “compatibility view” enabled
Java	Current 32-bit version of Java J2SE™ Runtime Environment
Reader	Current version of Adobe Reader
System Recovery	Full Operating System Recovery Package, Ensure the PC manufacturer or reseller provides the necessary recovery software to restore the operating system in the event of a major software failure.
Desktop Anti-Virus	Enterprise Desktop Anti-virus solution that is updated automatically and managed through a centralized console.

Minimum:	
Word Processing	MS Office Viewer
Spreadsheets	MS Office Viewer
Presentation	MS Office Viewer
Web Browser	Internet Explorer, version IE11 (with current Service Pack) with the “compatibility view” enabled
Java	Current 32-bit version of Java J2SE™ Runtime Environment
Reader	Current version of Adobe Reader
System Recovery	Full Operating System Recovery Package, Ensure the PC manufacturer or reseller provides the necessary recovery software to restore the operating system in the event of a major software failure.
Desktop Anti-Virus	Enterprise Desktop Anti-virus solution that is updated automatically and managed through a centralized console.

IT Service Continuity Management

IT Service Continuity Management is concerned with managing a dealership's ability to continue to provide a pre-determined and agreed level of IT services to support the minimum business requirements, following an interruption to the business. This includes:

- Ensuring business survival by reducing the impact of a disaster or major failure
    - Procuring backup or spare equipment of critical infrastructure elements such as the network gateway, switches or routers that if failed could impact network operations.
    - Configuring spare equipment in "high availability" for immediate failover in case of device malfunction or failure.
    - Eliminating "single points of failure" on the network by providing redundancy or high availability when possible.
    - Malware analysis using sandboxing technology.
- Reducing the vulnerability and risk to the business by effective risk analysis and risk management
- Preventing the loss of Customer and User confidence
- Producing IT recovery plans that are integrated with and fully support the dealership's overall Business Continuity & Disaster Recovery Plans
    - All key servers and hosts of Dealer must utilize automated and encrypted full Bare Metal Recovery off-site system recovery services.
    - System Recovery Package must allow for at least a 28-day recovery window and be stored within SSAE16 SOC-1 Type II compliant data centers. An additional encrypted local copy of the backups to speed restoration times is further recommended.
    - The Bare Metal Recovery should at a minimum be recoverable to the original host and preferably also to cloud recovery targets.
    - All backup events must be reviewed daily for failures or significant changes with prompt corrective action when necessary. Monthly reports summarizing the previous month's activities should be kept and reviewed by Dealer.

DIGITAL SIGNAGE INITIATIVE

** Configuration and settings are specific to Digital Signage and are NOT related to GlobalConnect, Service Department or other application settings.*

	SYSTEM CONFIGURATION
Standalone TV	**Recommended**: Commercial Grade HD TV that operates 24/7. Some recommended models: NEC (V552, P553, P703, P801, V652, V801) Samsung (ED75, ED65, DH55, DB75E, DB55E) **Minimum**: Consumer Grade HD TV with HDMI input.
Digital Media Player	**Required:** **Cisco Edge 340 Digital Media Player provided by GM**
Internet Connection – Wired	**Recommended:** Hardwired Ethernet Connection - Dedicated Internet access with 5 Mbps or higher bandwidth The following firewall internet ports must be open to enable your GM Digital Signage solution: 80, 443, 5228, 5220 and 5230. To confirm contact your Network Administrator.
Internet Connection - Wireless	**Optional:** Wireless connections must be on dedicated digital signage wireless networks as to not be in competition with dealer or guest network traffic. Bandwidth will be slower than a dedicated line but should target 5 Mbps. If the Wireless connection is weak or unstable, it may cause disruptions to the Weather and News feed services. Wireless networks should be established using the "Recommended" criteria defined in the wireless network section of this document and if using the WPA2 Enterprise Security for authentication, we recommend that the SSID is "Broadcast" and not "Hidden."
Web Browser	**Required:** To access and manage content from the GM Digital Signage Admin site, Google Chrome, Firefox and Internet Explorer version 11 are supported browsers.

Reference the "GM Digital Signage Reference Guide" for additional information and set-up instructions.

LOCAL AREA NETWORK (LAN) CONFIGURATION

Local Area Network	Ethernet based 1 Gigabit
Data Cabling	Existing data network cabling should be at a minimum category 5e. GM recommends a minimum of Category 6a for new cabling. Based on cabling run length, a repeater or fiber optic links may be necessary
Equipment Location	LAN wiring should terminate, and equipment should be housed, in a wiring closet or communications room
IP Addressing	Dynamic addressing (DHCP) should be used to ease support
Network Adapter	1 Gigabit
Traffic Switching	1 Gigabit Managed switch
Routers	Business-grade router
Unified Threat Management System (UTM)	Fully-managed security device that continually monitors threats through Intrusion Detection System “IDS” and Intrusion Prevention System “IPS” and other mechanisms such as packet filtering, anti-virus and stateful packet inspection

WIRELESS NETWORK

Note: When utilizing wireless networks, follow security Guidelines below. Wireless networks must be segmented from the dealership's wired LAN to protect customer data. It is recommended that dealers monitor all wireless internet traffic, limit usage and segment traffic in order to provide for optimized wireless network functionality and security.

Recommended: **Guidelines for implementing new systems**	
Network Standard	WPA2 Enterprise, 802.11N or 802.11AC with RADIUS authentication
Authentication & Encryption	WPA2 Enterprise, 802.11N with RADIUS authentication and AES Encryption
Coverage / Access Points	Wi-Fi should be accessible within the entire dealership footprint (including entire lot)

Minimum: **Lowest Acceptable Infrastructure for systems already in use at the dealership**	
Network Standard	WPA2 PSK Compliant
Authentication & Encryption	WPA2 Authentication w/ AES Encryption
Coverage / Access Points	Wi-Fi should be accessible within the entire dealership footprint (including entire lot)

Service Dept. Note:
The MDI and MDI 2 tools do not support RADIUS authentication; however, it is still possible to implement WPA2 Enterprise (i.e. 802.1x/802.11N) and WPA2 pre-shared key on the same network. This can be accomplished through network segmentation. This allows for a more secure WPA2 Enterprise solution that incorporates RADIUS as an authentication mechanism.

The MDI and MDI 2 are not compatible with an open, unencrypted wireless network.

Wireless Access Points:

GM supports business grade access points only and does not support Small Office/ Home Office equipment. All access points must adhere to the Guidelines specifications above. Please follow the link to the GMDIT.com site under products or GMDESolutions.com under Techline IT Solutions.

Rogue Wireless Detection:

- Scan, identify, and remove any rogue wireless access points that may be on the dealerships network. A rogue wireless access point is defined as a wireless point of entry into the dealership network that has is not authorized, secured, or known about by dealer IT, management, and ownership.
    - All rogue wireless networks must be detected, found, and removed immediately.
    - GM recommends the use of a managed wireless detection service that is continuously scanning the network for wireless threats.

SECURITY

PC Virus Monitoring

Enterprise-grade anti-virus products should be installed on all PCs and configured to automatically perform the following:

- Download and install most current virus signature updates
- Actively monitor for viruses
- Quarantine and eradicate infected files
- Anti-virus solution should include anti-virus, anti-spyware, intrusion prevention, application control, spam control and rootkit detection

Patch Management

GM recommends that patch management needs to be performed on every PC to ensure each workstation has current Microsoft patches. Workstation Management should include remote monitoring of hardware/software failures, down servers, low disk space, excessive CPU usage and excessive memory usage.

Email Security

- Outbound Email Security: Identify and respond to malware, inappropriate emails, unauthorized content, and company-private information before it leaves the network.
- Inbound Email Security: Apply filters to stop malware, phishing, or malicious emails before entering the network
- Encryption: TLS Email encryption is recommended in order to make it more difficult for third parties to read email in transit

Disaster or Attack Recovery

Essential dealership data should be backed up and verified regularly, using a backup service that has the following capabilities:

- Offsite secured storage of media
- Regular daily backups along with daily reviews of all system recovery events
- Monthly reports summarizing the previous month's activities should be kept and reviewed by the Dealer

Data Network Security

Comply with all federal, state, local, and industry regulations for financial institutions, such as GLBA, PCI, etc.

Designate an employee (dealer direct possibly your PSC) to be in charge of security policies, procedures, and FTC required paperwork. The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions regularly perform a Risk Assessment to identify foreseeable risks.

Network security monitoring, management and response: Proactive, real-time event monitoring that utilizes a SIEM (Security Information and Event Management) service. The service should be used for security information and event management to collect connected device data with the capability to aggregate and correlate varying security log data in real-time. The dealership must be aware of security events and anomalous behavior on the network, be able to respond and remediate immediately as well as provide the proper documentation for compliance purposes. The ultimate purpose of dealer network security management, monitoring and response is to aid in identifying or preventing an intrusion into the network and prove due diligence all while mitigating risk. Immediate response to a breach can greatly reduce or prevent data loss.

Note: Reactive management software (i.e. Desktop firewall or antivirus) is not to be confused with a proactive SIEM service.

Data Network Security (continued)

Implement comprehensive security measures that include:

- Fully-managed security device that continually monitors threats through Intrusion Detection System "IDS" and Intrusion Prevention System "IPS" and other mechanisms. The fully-managed security device should include the functionality listed below.
    - Filter packets and protocols
    - Antivirus Scanning
    - Perform stateful inspection of connections
    - Perform proxy operations on selected applications
    - Report traffic allowed and denied by the security device on a regular basis (i.e. monthly)
- The security device should be able to filter packets based on the following characteristics:
    - *Protocol, e.g. IP, ICMP
    - Source and destination IP addresses
    - Source and destination ports
    - The appliance should perform real-time scanning of HTTP, SMTP, and FTP traffic for malware, spy ware, and other intrusions.
    - In addition, GM recommends web filtering and monitoring websites visited to block inappropriate or entertainment orientated websites that are the most dangerous source for inadvertently downloading malicious programs.
- Timely, customized reporting on (IDS and IPS) activity
- Respond to all identified threats (form reporting) immediately.
- Protect each PC with unique passwords and a corporate anti-virus solution.
- GM recommends quarterly internal and external penetration testing and vulnerability scanning of the dealer network. A penetration test ("pen test") is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. A vulnerability scan is the process of identifying, quantifying and prioritizing the vulnerabilities in a system
    - A penetration test should be performed on any computer system that is to be deployed in a networked environment, in particular those with any Internet facing or exposed system.
    - GM recommends these types of tests/scans should be performed quarterly in order to proactively ensure the integrity of the network.

For additional information on Network Security, please reference the following resources that provide industry laws, Standards, and recommendations:

PCI Security Standards: https://www.pcisecuritystandards.org
Gramm-Leach-Bliley Act: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
STAR Standard: http://www.starstandard.org/

MINIMUM INTERNET BANDWIDTH

DEALER NETWORK SIZE	GUIDELINE
SMALL (under 20 PCs)	**16.0 Mbps download (total bandwidth), 3 Mbps upload**
MEDIUM (21 - 50 PCs)	**50.0 Mbps download (total bandwidth), 10.0 Mbps upload**
LARGE (Over 50 PCs)	**100.0 Mbps download (total bandwidth), 10.0 Mbps upload**

Note: GM recommends that dealerships also maintain on-demand backup Internet connectivity. GM recommends a backup or failover circuit in the event your primary goes down or if you choose to balance your traffic over two connections to streamline efficiency. When considering a backup connection, it is wise to make sure it comes from not only a different provider, but from a different backbone, as well.

Internet Notes

- Inefficient bandwidth may result in unreliable or slow performance and may negatively affect GM application speed and functionality.
- Internet speed and performance can be greatly impacted by virus, spyware and malware malicious infiltrations.
- Bandwidth-dependent activities not related to dealer/GM communications can greatly impact Internet performance as well. Examples of these activities are non-business Internet usage, i.e. video/audio downloads/uploads, gaming, file-sharing, etc.
- DMS communication requirements can also utilize significant amounts of bandwidth. Each dealer solution should consider the overall Internet utilization requirements for each area of the dealership. Additionally, dealers should develop Internet usage Guidelines for their employees that address non-dealership business Internet usage.

GM Dealerships, not General Motors Company, are ultimately responsible for determining their own network infrastructure, security, and network configuration.

Section 3: Appendix A

Techline Application Security and Firewall Exceptions

All application updates and installations must be performed from an account with local Windows administrative privileges.

Firewall Exceptions for TIS2Web applications:

- 64 bit Windows:
  - C:\Program Files (x86)\Java\jre<version number>\bin\jp2launcher.exe
  - C:\Program Files (x86)\GDS 2\jre6\bin\javaw.exe
  - C:\Program Files (x86)\General Motors\Tech2Win\bin\emulator.exe
  - C:\Program Files (x86)\GM MDI Software\GM MDI Manager\GM_MDI_Manager.exe
  - C:\Program Files (x86)\GM MDI Software\GM MDI Identification Service\GM_MDI_Ident.exe
  - C:\Program Files (x86)\General Motors\TIS2Web\TDS\tds.exe
  - C:\Program Files (x86)\Vibe Programming\Cuw.exe

- 32 bit Windows:
  - C:\Program Files\Java\jre<version number>\bin\jp2launcher.exe
  - C:\Program Files\GDS 2\jre6\bin\javaw.exe
  - C:\Program Files\General Motors\Tech2Win\bin\emulator.exe
  - C:\Program Files\GM MDI Software\GM MDI Manager\GM_MDI_Manager.exe
  - C:\Program Files\GM MDI Software\GM MDI Identification Service\GM_MDI_Ident.exe
  - C:\Program Files\General Motors\TIS2Web\TDS\tds.exe
  - C:\Program Files\Vibe Programming\Cuw.exe

Java Control Panel Security URL Exception:
- https://tis2web.service.gm.com

Internet Explorer Trusted Sites URL Exceptions:
- *.gm.com