



GM DEALER INFRASTRUCTURE GUIDELINES (DIG)

Version 21.2

The GM Dealer Infrastructure Guidelines have been designed to outline the dealership technology needed to ensure seamless and reliable dealer data communications and develop customers for life through efficient and effective systems and solutions.

GM DIG Version 21.2 May 2021

TABLE OF CONTENTS

1. Overview and General Notes	2
a. Overview	2
b. General Notes	2
2. Dealer Infrastructure	2
a. Endpoints	3
i. Hardware	3
ii. Software	7
b. LAN/Wi-Fi	8
i. Local Area Network (LAN)	9
ii. Wi-Fi	10
c. Transport (Bandwidth)	13
d. Security	14
i. Gateway Security (Firewalls & Unified Threat Management - UTM)	14
ii. Desktop Security	15
iii. Data Security	17
iv. Techline Application Security and Firewall Exceptions	19
e. Disaster Recovery and Business Continuity	22
i. Overview	22
ii. Risk Analysis & Mitigation	23

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://DESdealerservices.com> (1.800.GM.TOOLS) or Techline @ 800.828.6860 prompt Service.

1. OVERVIEW AND GENERAL NOTES

A. OVERVIEW

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 help ensure a seamless and reliable conduit for GM to dealer data communications. These guidelines also outline dealership related systems, solutions and technology needed to assist with creating customers for life. GM Dealerships, not General Motors LLC, are ultimately responsible for determining their own network infrastructure, security, and network configuration.

B. GENERAL NOTES

The infrastructure guidelines are organized as follows:

- **Good** – the minimum acceptable systems capability/components for conducting business with GM
- **Better** – the systems infrastructure capability/components that will deliver better performance and security while seeking to maximize the lifecycle of the investment.
- **Best** – the systems infrastructure capability/components that will deliver best performance and security while seeking to maximize the lifecycle of the investment.



NOTE: If you are looking to purchase new infrastructure, systems or solutions, please adhere to the specifications outlined in the “Better or Best” sections.

2. DEALER INFRASTRUCTURE

A dealership's network infrastructure consists of the Endpoint (hardware and software) resources used to enable network connectivity, communication, operations, and management of the dealer's local area network (LAN). Network infrastructure provides the communication path and services between Dealers, service providers, GM, and end customers. Proper selection and implementation of network infrastructure are critical to ensuring network efficiency and compatibility with GM, DSP, and dealership applications/data.

A. ENDPOINTS

Any interface/device used to communicate with systems and solutions.

I. HARDWARE

Dealership hardware is a physical device that serves the purpose of capturing dealer data (PCs, laptops, handheld devices), routing that data (routers, switches, firewalls), and providing that data when needed (servers, monitors, and peripherals).

Selection of network hardware is a critical component of managing a dealership's network. While new hardware can be a considerable capital expenditure, it is important to understand that there is also a considerable cost associated with old hardware as it can significantly hinder business operations because of speed or compatibility issues, for example.

The following section details when to purchase new hardware, guidelines for purchasing, and recommendations for purchasing desktops, laptops, and routing equipment.


Consumer-Grade versus **Enterprise-Grade**: Most computer Manufacturer's offer two different grades of computers: consumer-grade hardware intended for home and personal use, and enterprise-grade hardware intended for businesses. While the price of consumer-grade hardware may seem attractive for dealerships, oftentimes the total cost of ownership ends up being greater due to the limited functionality, higher failure rates, and more complex support.

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

SUPPORTED	NOT SUPPORTED
Enterprise grade hardware (PCs and Access Points)	Consumer grade hardware (PC and Access Points), Apple or Mac tablets & PCs Non-branded, built by hand or thin client PC
Intel Core i3 / i5 / i7 processors 6 th generation and above	ALL Intel Core i-series 5 th generation and below Processors plus AMD, Celeron, Pentium and Atom processors
Windows 10 Professional, 64 bit	Windows 8.x, XP and Vista Business Windows7 Professional, 32 and 64 bit All Home Operating Systems Tablets running Android or Mac operating systems
Java Run Time Environment 32 bit	All 64 bit versions of Java

1. DESKTOP PC

	Good	Better	Best (& Servers)
Processor	Intel Core i3, i5, i7 6th & 7th Gen	Intel Core i3, i5, i7 8th Gen	Intel Core i5, i7 9th Gen* & above Server: Intel Dual Core Xeon or better
System memory (RAM)	8GB	16GB	16GB
Hard Disk Drive (HDD or SSD)	**256 GB +	500 GB +	1TB +
CD / DVD Drive	CD/DVD Combo	CD/DVD Combo	CD/DVD Combo
USB A 2.0 & 3.0	2+	2+	2+
Display	20" 1366 x 768 (HD)	22" 1920 x 1080 (FHD)	24" 1920 x 1080 (FHD)
Network Adapter	Wired: Gigabit Wireless: 802.11ac	Wired: Gigabit+ Wireless: 802.11ac	Wired: Gigabit+ Wireless: 802.11ax
Operating System	Windows 10 Professional, 64 bit	Windows 10 Professional, 64 bit	PC: Windows 10 Professional, 64 bit Server 2012: Std. & Ent. editions
Warranty	3 Year on site	3 Year on site	3 Year on site

 *Note: 8th Generation or above have model numbers of 8000 or greater (example: Intel Core i5-8500).*
Note: For Service Technicians who perform Infotainment programming the 256GB drive size is not sufficient for large calibration files. Select from the Better or Best category.

When using for EPC (Electronic Parts Catalog):

- 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.

US & Canada	Holden	Mexico	International	South America	Brasil
350 GB	200 GB	250 GB	600 GB	250 GB	175 GB

- To ensure proper function of the GM EPC, internet content filters should be updated to allow *.epclink.com.

Note: Hardware that doesn't meet the "Better" specifications may not be supported by Snap-on upon contract renewal.

Note: Use of any remote connection services, including but not limited to RDP (Windows Terminal Services), VNC, Teamviewer, ShowMyPC, Chrome Remote Desktop, etc. is not authorized or supported for GM EPC users. This also includes running the application on server operating systems in Cloud hosting configurations. The EPC application runs on a single physical machine with one concurrent user.

For the Techline Service Technician applications (Techline Connect, TIS2Web, GDS2, MDI Manager, MDI / MDI 2, Tech2Win, Data Bus Diagnostics Tool and Service Information):

- **Requires Local Windows Administrative access for software installation and updates to Windows registry**
- Refer to section 2.d.iv and 2.d.v for a list of recommended firewall and security exceptions plus an alternative to full admin rights
- Recommend one (1) laptop for each technician performing service programming and vehicle diagnostics, otherwise, one for every two technicians
- Recommends one (1) Multiple Diagnostic Tool (MDI 2) for every Techline PC
- Recommends one (1) battery maintainer for every two (2) Multiple Diagnostic Interface (MDI) tools in use
- Recommends use of Tripp-Lite Keyspan USB to Serial adapter (Model: USA - 19HS) for computers without serial ports

2. LAPTOP & TABLET PC'S

	Good	Better	Best
Processor	Intel Core i3, i5, i7 6th & 7th Gen	Intel Core i3, i5, i7 8th Gen	Intel Core i5, i7 9th Gen* & above Server: Intel Dual core Xeon or better
System memory (RAM)	8GB	16GB	16GB +
Hard Disk Drive (HDD or SSD)	**256 GB +	500 GB +	750 GB +
CD / DVD Drive (optional/external)	CD/DVD Combo	CD/DVD Combo	CD/DVD Combo
USB A 2.0 & 3.0	2+	2+	2+
Display	13" 1366 x 768 (HD)	15" 1920 x 1080 (FHD)	15+" 1920 x 1080 (FHD)
Network Adapter	Wired: Gigabit Wireless: 802.11ac	Wired: Gigabit+ Wireless: 802.11ac	Wired: Gigabit+ Wireless: 802.11ax
Operating System	Windows 10 Professional, 64 bit	Windows 10 Professional, 64 bit	Windows 10 Professional, 64 bit
Warranty	3 Year on site	3 Year on site	3 Year on site



* Note: 8th Generation or above have model numbers of 8000 or greater (example: Intel Core i5-8269U).

** Note: For Service Technicians who perform Infotainment programming the 256GB drive size is not sufficient for large calibration files. Select from the Better or Best category.

The area of usage should be considered when purchasing laptop or tablet PC. If device will be used in the service department, a rugged case design should be considered.

For the Techline Service Technician applications (Techline Connect, TIS2Web, GDS2, MDI Manager, MDI / MDI 2, Tech2Win, Data Bus Diagnostics Tool and Service Information):

- **Requires Local Windows Administrative access for software installation and updates to Windows registry**
- Refer to section 2.d.iv and 2.d.v for a list of recommended firewall and security exceptions plus an alternative to full admin rights
- Recommends one (1) laptop for each technician performing vehicle diagnostics, otherwise, one for every two technicians
- Recommends one (1) Multiple Diagnostic Tool (MDI 2) for every Techline PC
- Recommends one (1) battery maintainer for every two (2) Multiple Diagnostic Interface (MDI) tools in use
- Recommends use of Tripp-Lite Keyspan USB to serial adapter (Model: USA – 19HS) for computers without serial ports

3. TABLETS & MOBILE DEVICES

Tablets are handheld devices designed for mobility and accessibility. Tablets don't have the same functionality as a desktop or laptop machine. Because of this, it is highly recommended that dealerships do not replace desktop or laptop PCs with tablets, but rather augment with tablets when application and function call for greater mobility and accessibility.

Some GM applications are specifically developed to run on certain tablet devices, such as iPads. When these applications are deployed, GM will communicate for 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.

II. SOFTWARE

Software is the program or operating information used by the dealership hardware to capture, store, manipulate, and display data on network hardware. Dealerships use software to capture customer data, automate business processes for selling and servicing vehicles, and communicate with other systems or networks.

	Good	Better	Best
Word Processing	Microsoft World Mobile	Microsoft Word Mobile	Office 365 ProPlus
Spreadsheets	Microsoft Excel Mobile	Microsoft Excel Mobile	Office 365 ProPlus
Presentation	Microsoft PowerPoint Mobile	Microsoft PowerPoint Mobile	Office 365 ProPlus
Microsoft Teams	Web or Mobile version for use in the Technician Service Bay. Technicians may be asked to use MS Teams while troubleshooting with Technical Assistance or Field Service Engineering .		
Web Browser	Internet Explorer, version IE11 (with current Service Pack) with the "compatibility view" enabled See Note below regarding Microsoft Edge		
Java	Current 32-bit version of Java Runtime Environment, or the version recommended by each application		
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. (Note: See Business Continuity Section)		
Desktop Anti-Virus	Enterprise Desktop Anti-virus solution that is updated automatically and managed through a centralized console.		

Note: As of October 2020, Microsoft will continue to support Internet Explorer 11 as a web browser for the duration of Windows 10. This is subject to change as Microsoft sees fit, and for the latest updates you can reference this website: <https://docs.microsoft.com/en-us/lifecycle/faq/internet-explorer-microsoft-edge>. As Microsoft has announced, a shift to Microsoft Edge is under way. GM is working to make sure all applications function in Edge and at some point, Edge will be the primary browser.

B. LAN/WI-FI

A local area network (LAN) is a group of computers and associated devices connected together using shared common communications such as cable line or wireless link. Dealerships must manage a network so devices at the dealership can effectively but securely communicate and share resources.

Network management can be a difficult task for auto dealers. Dealers need to make the network available to share data as well as limit access for security purposes. Besides dealership employees, oftentimes a service provider, the OEM and its representatives, and even customers may also need to share the network resources. Providing safe and secure access to the dealership network can be challenging.

The section that follows provides recommendations for local area network configuration and management. It also provides advice on wireless networking, dealership mobility, and customer access.

I. LOCAL AREA NETWORK (LAN)

	Good	Better	Best
Local Area Network	Ethernet based 1 Gigabit	Ethernet based 1 Gigabit	Ethernet based 1 Gigabit
Data Cabling	Cat-5e	Cat-6	Cat-6a
	Fiber optic cable is highly recommended in place of data cable runs when the length exceeds 295 feet (90 meter)		
Equipment Location	Locked Room	Locked & Clean Room	Locked, Clean & Temp. Control
	LAN wiring should terminate & equipment should be housed in a wiring closet or communications room		
IP Addressing*	Dynamic addressing (DHCP)	Dynamic addressing (DHCP)	Dynamic addressing (DHCP)
Network Adapter	1 Gigabit	1 Gigabit	1 Gigabit
Traffic Switching	1 Gigabit Managed switch	1 Gigabit Managed switch	1 Gigabit Managed switch
Routers	Enterprise-grade router. Routers should support Network Address Translation/Process Analytical Technology (NAT/PAT). Routers should also support dynamic routing using RIPv2, OSPF and BGP. - Change the device password at the time of installation and on an ongoing, regular basis. - Keep backup configuration on file in the case of a software failure or hardware replacement.		
Network Gateway	See Firewall/ UTM section of this document (Section D, Firewall/UTM)		
Domain Name Services (DNS)	Use public DNS except when using Windows Active Directory. (In which case, having an internal DNS server is required.)		

*IP Addressing: In some situations, dealerships may be required to obtain a static IP from their ISP for DMS or other 3rd party vendor communications.

	Good	Better	Best
Ethernet Standard Specification	IEEE 802.3 100baseT	IEEE 802.3 1000baseT	IEEE 802.3 1000baseT
Redundancy	The connection of multiple switches together should use redundant links of the highest speed available, using STP or rSTP to ensure a loop-free topology.		
Power Supply	Redundant power supplies are recommended to reduce downtime.		
Speed	100 Mbps	1000 Mbps	1000 Mbps
VLAN	Switches with VLAN and 802.1Q trunk technology should be used for routed networks with multiple subnets or VLANs.		
Networking Between Locations	IPSec or SSL VPN Technology should be used for encrypted, secure data transmission between dealership locations		SD-WAN
Management Protocols	Managed devices should support industry remote management standards such as Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).		
Wireless Access Points	Dual Band IEEE802.11AC	Dual Band IEEE 802.11ac or better	Dual Band IEEE 802.11ax or better

II. WI-FI

Wireless LANs enable network communication without the physical restraints of hard-wired cabling. Wireless technology can be especially convenient in that it can provide mobility to employees, allow customers to bring and use their own device, and expand the dealer network beyond the physical walls of the dealership. Dealers should also understand with the ubiquity of wireless networks comes challenges around design, support, and security.

	Good	Better	Best
Network Standard	802.11AC with RADIUS authentication	802.11AC with RADIUS authentication	802.11ax with RADIUS authentication
Authentication & Encryption	WPA2 Authentication w/ AES Encryption	WPA2 Enterprise with RADIUS authentication and AES Encryption	WPA2 Enterprise with RADIUS authentication and AES Encryption
Guest Network Access	Guest network wireless access is configured to be separate from production network and access passwords are changed every 90 days. The wireless network is disabled after business hours. Blocks are enabled to prohibit illegal file sharing (eg. BitTorrent, limewire, etc.).	Guest network wireless access is configured to be separate from production network and access passwords are changed every 90 days. The wireless network is disabled after business hours. Blocks are enabled to prohibit illegal file sharing (eg., BitTorrent, limewire, etc). In addition, access to the guest wireless network is configured to not exceed the perimeter of the dealership premises.	Guest wireless access is first redirected to a Guest wireless registration page where the guest agrees to acceptable use policy and receives a one-time password before being granted access to Guest network.
Wireless Coverage	Business Coverage includes: sales showroom, service drive, service shop and customer lounge. Guest Coverage includes: sales showroom, service drive, service shop and customer lounge.	Business Coverage includes: sales showroom, service drive, service shop, customer lounge and vehicle lot. Guest Coverage includes: sales showroom, service drive, service shop, customer lounge and vehicle lot.	Business Coverage includes: sales showroom, service drive, service shop, customer lounge, service lot and vehicle lot. Guest coverage includes: sales showroom, service drive, service shop, customer lounge, service lot and vehicle lot.
Wireless Hardware	Only enterprise-grade access points should be used. Enterprise grade access points are designed to provide roaming and other business class features (such as VLANs and/or multiple SSIDs) necessary to support the wireless devices for applications. Enterprise grade wireless access points are also designed to accommodate a higher number of connections than consumer-grade hardware.		
Network Segmentation	Dealerships must ensure guest traffic is segmented from the dealership network through VLANs or a separate internet connection.		
SSIDs	Dealerships are recommended to use separate SSIDs for different business functions (i.e. sales, service, and administration). However, dealerships should not confuse SSIDs with network segmentation. SSIDs generally do not separate network traffic, but only provide a different way to join the network.		

Rogue Wireless Detection	<p>Continuously Scan, identify and remove any rogue wireless access points that may be on the dealership's network.</p> <p>-A rogue wireless access point is defined as a wireless point of entry into the dealership's network that has not been authorized or secured by the dealer or any unauthorized wireless access point using the production SSID's (mimicking a production AP).</p> <p>-All rogue wireless networks must be detected, found, and removed immediately.</p>

Service Dept. Note:

WPA2 authentication is *required* for Service Advisor Vehicle Interface (*SAVI) to function. WPA and WEP will not be supported.

Note: SAVI is available to United States Dealerships only.

Dealership Mobility	
Recommendations	Specification
Mobility within the dealership	Utilize a wireless mesh network to ensure end users can navigate around the location without losing connection or authenticating again.
Wireless controllers	A wireless LAN controller can be used in combination with the Lightweight Access Point Protocol (LWAPP) to manage lightweight access points across the dealership network. This will help to ensure adequate coverage, reliability, and network efficiency.

Customer Access	
Recommendations	Specification
Traffic Prioritization	Dealerships should utilize a firewall or other mechanism to limit guest bandwidth consumption. This will prevent guest access from interfering with business operations by consuming too much bandwidth.
Guest Authentication/ Terms of use	GM recommends dealerships utilize a captive portal requiring guests to accept terms and conditions of use at the dealership. This can include content restrictions, bandwidth limitations, and usage agreements.

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. 802.11ac/802.11ax) 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.

SAVI requires an access point within 130 feet of every point within the service lane if using 2.4Ghz frequency band and 65 feet if using 5Ghz. Access points should be within line-of-sight.

C. TRANSPORT (BANDWIDTH)

Internet bandwidth is the amount of data that can be sent to and from the dealership, usually measured in bits per second. Most dealership software relies on the internet for data communication. Inventory information, work orders, service manuals, and vehicle data are often accessible via the internet. Also, many employees and customers rely on the dealership’s internet access for personal reasons such as to check email or surf the web. Since so many users depend on the internet for information, it is critical that the dealership procures enough bandwidth to adequately provide each resource with enough bandwidth to quickly access data. To ensure the dealership has enough bandwidth, a dealer must choose the right technology and speed.

Dealer Network Size	Good	Better	Best
Small (Under 20 Endpoints)	16 Mbps download (total bandwidth), 3 Mbps upload	Bandwidth speeds meet “good” criteria Dealership utilizes a backup internet connection	Bandwidth Speeds meet “good” criteria Dealership utilizes a backup internet connection with Auto Failover Capabilities
Medium (21 – 50 Endpoints)	50.0 Mbps download (total bandwidth), 10.0 Mbps upload	Bandwidth speeds meet “good” criteria Dealership utilizes a backup internet connection	Bandwidth Speeds meet “good” criteria Dealership utilizes a backup internet connection with Auto Failover Capabilities
Large (Over 51 Endpoints)	100.0 Mbps download (total bandwidth), 10.0 Mbps upload	Bandwidth speeds meet “good” criteria Dealership utilizes a backup internet connection	Bandwidth Speeds meet “good” criteria Dealership utilizes a backup internet connection with Auto Failover Capabilities



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.

- 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.

D. SECURITY

The purpose of a dealership’s network infrastructure is to share data and resources with employees, customers, and third-party vendors or partners. Dealerships must also take steps to ensure this data is shared securely. Dealerships should monitor both known and unknown connections for signs of data loss. A dealership must take measures to protect data at the gateway and each endpoint of the network. Technologies, processes, and procedures must be utilized to ensure dealer data does not end up in the wrong hands.

I. GATEWAY SECURITY (FIREWALLS & UNIFIED THREAT MANAGEMENT - UTM)

	Good	Better	Best
Firewall/ Unified Threat Management (UTM)	<p>A fully-managed Unified Threat Management (UTM) appliance that continually monitors threats through Intrusion Detection system “IDS” and Intrusion Prevention System “IPS” and other mechanisms.</p> <p>The device should also have the following features:</p> <ul style="list-style-type: none"> • Mechanisms such as packet filtering, antivirus, and stateful packet inspection. • Filter packets and protocols (e.g. IP, ICMP) • 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) • IP Content Filtering 	<p>A fully-managed Unified Threat Management (UTM) appliance that continually monitors threats through Intrusion Detection system “IDS” and Intrusion Prevention System “IPS” and other mechanisms.</p> <p>The device should also have the following features:</p> <ul style="list-style-type: none"> • Mechanisms such as packet filtering, antivirus, and stateful packet inspection. • Filter packets and protocols (e.g. IP, ICMP) • 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) • URL content Filtering <p>Procure backup Firewall/UTM appliance to be deployed in the case of hardware failure.</p>	<p>A fully-managed Unified Threat Management (UTM) appliance that continually monitors threats through Intrusion Detection system “IDS” and Intrusion Prevention System “IPS” and other mechanisms.</p> <p>The device should also have the following features:</p> <ul style="list-style-type: none"> • Mechanisms such as packet filtering, antivirus, and stateful packet inspection. • Filter packets and protocols (e.g. IP, ICMP) • 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) • Log inspection looking for anomalous activity to botnets or other malicious sites. • Network gateway utilizes sandboxing technology to monitor and test dealership network traffic. • Utilize category content filtering <p>Procure backup Firewall/UTM appliance. Install in high availability configuration for auto failover in the case of primary device failure.</p>

Network Segmentation	Payment Card information, customer information, dealership traffic, and customer traffic should be segmented via network segmentation (such as VLAN) or a different network (such as a dedicated circuit for guests) to ensure data security.		
Content Filtering	Dealerships utilize IP Content Filtering	Dealerships utilize URL Content Filtering	Dealerships utilize category Content Filtering

II. DESKTOP SECURITY

	Good	Better	Best
PC Virus Monitoring	<p>Enterprise-grade, antivirus products should be installed on all PCs and configured to automatically perform the following:</p> <ul style="list-style-type: none"> • Download and install most current virus signature updates • Actively monitor for viruses • Quarantine and eradicate infected files • Antivirus solution should include antivirus, anti-spyware, intrusion prevention, application control, spam control and rootkit detection 		
Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR)	<p>A singular endpoint protection platform (EPP) and endpoint detection and response (EDR) solution must be deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. The service offering should provide cross-platform visibility into endpoint/server activities as well as:</p> <ul style="list-style-type: none"> • Threat Detection through static and behavioral AI engines and HIDS within the endpoint agent • Threat Containment • Activity Reporting and Threat Hunting • Log endpoint activity to a SIEM and retaining logs for a rolling 400 days • Cross Platform visibility into process execution, network communications, file access, applications, DNS requests and encrypted web traffic 	<p>A singular endpoint protection platform (EPP) and endpoint detection and response (EDR) solution must be deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. The service offering should provide cross-platform visibility into endpoint/server activities as well as:</p> <ul style="list-style-type: none"> • Threat Detection through static and behavioral AI engines and HIDS within the endpoint agent • Threat Containment • Activity Reporting and Threat Hunting • Log endpoint activity to a SIEM and retaining logs for a rolling 400 days • Cross Platform visibility into process execution, network communications, file access, applications, DNS requests and encrypted web traffic • 24x7x365 monitoring and response 	<p>A singular endpoint protection platform (EPP) and endpoint detection and response (EDR) solution must be deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. The service offering should provide cross-platform visibility into endpoint/server activities as well as:</p> <ul style="list-style-type: none"> • Threat Detection through static and behavioral AI engines and HIDS within the endpoint agent • Threat Containment • Activity Reporting and Threat Hunting • Log endpoint activity to a SIEM and retaining logs for a rolling 400 days • Cross Platform visibility into process execution, network communications, file access, applications, DNS requests and encrypted web traffic • 24x7x365 monitoring including alerting and response to potential threats via a SOC 2 certified

	<p>Note: PC Virus monitoring is not to be confused with EPP/EDR. An EDR/EPP will monitor all endpoints and critical servers for suspicious activity with the ability to quarantine endpoints infected with malware.</p>	<p>Note: PC Virus monitoring is not to be confused with EPP/EDR. An EDR/EPP will monitor all endpoints and critical servers for suspicious activity with the ability to quarantine endpoints infected with malware.</p> <p>24x7x365 monitoring and alerting and response to potential threats.</p>	<p>managed security service provider</p> <p>Note: PC Virus monitoring is not to be confused with EPP/EDR. An EDR/EPP will monitor all endpoints and critical servers for suspicious activity with the ability to quarantine endpoints infected with malware.</p> <p>24x7x365 monitoring and alerting and response to potential threats.</p>
Patch Management	<ul style="list-style-type: none"> • GM recommends that patch management be performed on every PC to ensure each workstation has current patches. • Workstation Management should include remote monitoring of hardware/software failures, down servers, low disk space, excessive CPU usage and excessive memory usage. Install critical security patches within one month of release. 		
Password Protection	<p>Employees have multiple user ID's and passwords used to access the tools that support user's job roles. Implementing a password management policy is a significant piece of data security and access control. All passwords should be promptly changed if suspected of/are being comprised, or disclosed to vendors for maintenance/support.</p> <ul style="list-style-type: none"> • Refrain from divulging passwords unless absolutely necessary (i.e., helpdesk assistance) • Protect stored passwords – discourage employees from writing down access information and keeping it in plain sight of passerby (i.e., username & password written on post it note nearby workspace). • Passwords should be encrypted when transmitted electronically. • Passwords must be changed every 90 days. • Users are not able to reuse their last five (5) passwords. • User accounts are locked-out or suspended after the tenth (10) failed login attempts. • Remove all employee credentials from all network devices immediately upon employment ending. 		

III. DATA SECURITY

	Good	Better	Best
Security Information Event Management (SIEM)	<p>Proactive, real-time security event monitoring that utilizes a SIEM (Security Information and Event Management) service. The SIEM service needs to be able to notify the network administrator in the case of a security event, as well as provide the proper documentation for compliance purposes. The ultimate purpose of a SIEM service is to aid in identifying or preventing an intrusion into your network. Immediate response to a breach can greatly reduce or prevent data loss.</p> <p>Note: Reactive management software (i.e. Desktop firewall or antivirus) is not to be confused with a proactive SIEM Service. UTM Firewalls is also not synonymous with SIEM technology. SIEM and UTM technologies work together to provide protection & monitoring of network traffic.</p>	<p>Proactive, real-time security event monitoring that utilizes a SIEM (Security Information and Event Management) service. 24x7x365 security event monitoring and response. The SIEM service needs to be able to notify the network administrator in the case of a security event, as well as provide the proper documentation for compliance purposes. The ultimate purpose of a SIEM service is to aid in identifying or preventing an intrusion into your network. Immediate response to a breach can greatly reduce or prevent data loss.</p> <p>Note: Reactive management software (i.e. Desktop firewall or antivirus) is not to be confused with a proactive SIEM Service. UTM Firewalls is also not synonymous with SIEM technology. SIEM and UTM technologies work together to provide protection & monitoring of network traffic.</p> <p>24x7x365 security event monitoring and response should include not only around the clock alerting, but immediate response to potential threats.</p>	<p>Proactive, real-time security event monitoring that utilizes a SIEM (Security Information and Event Management) service. 24x7x365 security event monitoring and response by a SOC 2 certified managed security service provider. The SIEM service needs to be able to notify the network administrator in the case of a security event, as well as provide the proper documentation for compliance purposes. The ultimate purpose of a SIEM service is to aid in identifying or preventing an intrusion into your network. Immediate response to a breach can greatly reduce or prevent data loss. This includes checking for anomalous outgoing connections including indications of Command and Control connections from internal systems to known botnets and other malicious sites.</p> <p>Note: Reactive management software (i.e. Desktop firewall or antivirus) is not to be confused with a proactive SIEM Service. UTM Firewalls is also not synonymous with SIEM technology. SIEM and UTM technologies work together to provide protection & monitoring of network traffic.</p> <p>24x7x365 security event monitoring and response should include not only around the clock alerting, but immediate response to potential threats.</p>
Penetration Testing and Vulnerability Scanning	Quarterly External Vulnerability Scanning	Quarterly External and Internal Vulnerability Scanning	Quarterly External and Internal Vulnerability Scanning Internal/ External Penetration Testing
Governance, Risk, and Compliance	Comply with all federal, state, local, and industry regulations for financial and retail 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. It is recommended that each dealership consult with their legal counsel for information related to all applicable laws and compliance.		

	PCI Security Standards: https://www.pcisecuritystandards.org Gramm-Leach-Bliley Act: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html		
File Integrity Management and Monitoring	Dealerships should utilize file integrity management & monitoring (FIM) solution to monitor data, changes, and movement	Dealerships should utilize file integrity management & monitoring solution to monitor data, changes, and movement.	Event logs from FIM solution should be sent to a SOC 2 certified managed security provider for 24x7x365 alerting and response
Email Security	<ul style="list-style-type: none"> • Outbound Email Security: Identify and respond to malware, inappropriate emails, unauthorized content, and dealer-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 in order to make it more difficult for third parties to read email in transit 		
Website Security	Perform regular website scanning and testing for vulnerabilities such as malware, backdoors, SQL injection and cross site scripting.		
Security Awareness Training	Develop and deploy an ongoing security awareness training program. Covering, but not limited to the following topics: <ul style="list-style-type: none"> • Security Documentation <ul style="list-style-type: none"> ○ Acceptable use Policy ○ Audit Policy ○ Extranet Policy ○ Password Policy ○ Wireless Standards and usage policy • Data Security Planning <ul style="list-style-type: none"> ○ Data Collection, Retention and Use ○ Security Incident Response Plan ○ Access Control • Audit and Review Processes <ul style="list-style-type: none"> ○ Risk Analysis ○ Reporting ○ Employee Education 		

IV. TECHLINE AND SERVICE ADVISOR VEHICLE INTERFACE APPLICATION SECURITY, FIREWALL EXCEPTIONS PLUS ALTERNATIVES TO LOCAL ADMIN RIGHTS

All application updates and installations must be performed from an account with local Windows administrative privileges. Firewall Exceptions for TIS2Web and Techline Connect applications:

- Application Exceptions:
 - C:\Program Files (x86)\TechlineConnect\tlc.exe
 - C:\Program Files (x86)\Techline Connect\jre\bin\javaw.exe
 - C:\Program Files (x86)\TechlineConnect\TDMWindowsService.exe
 - 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
- Java Control Panel Security URL Exception:
 - <https://tis2web.service.gm.com>
- Internet Explorer Trusted Sites URL Exceptions:
 - *.gm.com

The Service Advisor Vehicle Interface (SAVI) requires firewall exceptions:

- <https://cvpstageapi.danlawinc.com>
- <https://gmdealerservices.gm.com>
- <https://tla-mqtt.ext.gm.com>
- api.bitbrew.com
- ota.bitbew.com
- portal.bitbtrew.com

SAVI uses Ports:

- 443
- 8883

If your dealership already has privilege management software installed, the list in the table below is all you should need to configure **Techline Connect** to have the elevated privileges necessary.

Description	Type	File Name	Child Process
TLC - Data Bus Diagnostic Tool	Installer Package	Data Bus Diagnostic Tool.msi	Elevate All

TLC - Data Bus Diagnostic Tool	Exe	\\setup.exe	Elevate ALL
TLC - GDS 2 0624CA22-A85C-4A3B-97DD-C73ACB26AFEF	Installer Package	Any install with the app id in the description (0624CA22-A85C-4A3B-97DD-C73ACB26AFEF)	Elevate All
TLC - GM MDI Manager	Exe	"\\Program Files (x86)\\GM MDI Software\\GM MDI Manager\\setup.exe"	Elevate All
TLC - IVCS 5Byte Proxy	Exe	\\ivcs5bcp_install.exe	Elevate All
TLC - IVCS Cyber Proxy	Exe	\\ivcsbcp_install.exe	Elevate All
TLC - Medium Duty	Exe	\\MMUReaderInstall.exe	Elevate All
TLC - SPS2	Exe	\\sps2.exe	Elevate All
TLC - Setup Suite Launcher Unicode	Exe	\\TLCInstaller* Need to use wild card to elevate any TLCinstaller exe	Elevate All
TLC - TDM	Exe	\\TDM.exe	Elevate All
TLC - TIS2WEB Proxy	Exe	\\t2w_TLC_install.exe	Elevate All
TLC - TIS2Web IVCS5B COM Proxy.msi	Installer Package	\\TIS2Web IVCS5B COM Proxy.msi	Elevate All
TLC - Tech2WinSetup.exe	Exe	Tech2WinSetup.exe	Elevate All
TLC - TechLine Connect Installer	Exe	\\tlc*.exe (Wild card to catch tlc core, tlc extension and tlc)	Elevate All
TLC - certificate- GDS2 Installation	Exe	*Any exe signed with certificate "GDS2 Installation"	Elevate All
TLC – certificate – MAHLE Powertrain LLC	Exe	*Any exe signed with certificate "MAHLE Powertrain LLC"	Elevate All

TLC - c - Mahle Aftermarket Inc.	Exe	*Any exe signed with certificate "Mahle Aftermarket Inc."	Elevate All
TLC - regasm.exe	Exe	\regasm.exe	Elevate All

Use the information below to configure the **Service Advisor Vehicle Interface** device (SAVI) for elevated privileges.

SAVI Manager	Installer Package	ServiceLaneDongle_Setup.msi	Elevate All
--------------	-------------------	-----------------------------	-------------

I. OVERVIEW

Disaster recovery and business continuity refer to an organization’s ability to recover from a disaster and resume normal network operations. Dealerships should have a plan in place that details the technology, processes, and procedures to take in the case of a failure. The key to successful disaster recovery is to have a plan well before the outage occurs.

Disaster recovery and business continuity planning processes help organizations prepare for disruptive events, no matter how extensive (i.e. everything from a devastating tornado to a simply broken internet line caused by repeated freezing and thawing).

To understand what might happen in the case of a network failure, a dealership is encouraged to first understand what data is at risk. How long can that data be unavailable? What happens when it is unavailable? What steps can be performed to make sure that risk is mitigated? This section details some basic answers to those questions as well as some recommendations for planning for failure as well as restoring network operations.

	Good	Better	Best
Data Recovery	Network gateway configuration and critical data should be backed up and maintained in the case of network or hardware failures.	<p>Network gateway configuration and critical data should be backed up and maintained in the case of network or hardware failures.</p> <p>Dealership should have a documented disaster recovery plan covering the technologies and processes to ensure business continuity in the case of network or data failure.</p> <p>Dealerships should have at least a 28-day recovery window for all data. Data should be stored within SSAE16 SOC-1 Type II compliant data centers.</p> <p>Dealer backup data should be verified regularly with daily review of all system recovery events.</p>	Dealerships should meet the “good” and “better” criteria and perform scheduled DR tests/ drills against these technologies, documentation, and processes.

II. RISK ANALYSIS & MITIGATION

The main purpose of risk analysis is to help the dealership identify all the areas for which there may be a risk of loss. This can be hardware, software, building, personnel, etc. After the various items have been identified, the dealership can classify the level of each risk and determine how that risk affects the dealership.

Some of the various categories of risk with which a dealership may be faced are listed below.

- Key Personnel
- Building
- Key System Failure
- Total System Failure
- Data loss

There are various ways that an organization can mitigate risk. These plans or solutions can be either on-site or off-site. Some examples of each follow.

Onsite Risk Mitigation Options	Offsite Risk Mitigation Options
Redundant Hardware	Remote Back Up Software
Onsite Data Back Up Software and servers	Cloud Storage
Uninterruptible Power Supply (UPS)	RMA Hardware Service Contracts
Generators	