GM DEALER INFRASTRUCTURE & SECURITY GUIDELINES (DISG)

The GM Dealer Infrastructure and Security 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 DISG Version 2023.2, February 2023

CONTENTS

For questions related to the GM Infrastructure and Security 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

The purpose of these guidelines is to assist dealerships with implementing infrastructure and processes to provide a seamless and reliable conduit for dealership related systems, services, and security.

GM has adopted these infrastructure and security guidelines for the dealership's internal network environment in accordance with Article 5.6 of the Dealer Sales and Service Agreement. Each dealership has the responsibility to protect confidential information and determining their own network infrastructure, security, and network configuration. For purposes of these guidelines, confidential information is defined as dealer information and data that should not be accessible to anyone without a "need to know." Each dealership must ensure the security of customer information, including confidential information held on behalf of customer or clients.

Protecting dealership data means protecting its confidentiality, integrity, and availability. The potential consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company goodwill.

Dealer service providers, third parties, and General Motors cannot guarantee a secure dealer network, even if dealers follow the guidelines in this document. GM also recommends that dealerships turn to industry experts, industry, and federal guidelines and other knowledgeable resources for help with dealer data security.

United States Only: Note that these infrastructure and security standards can also apply to dealer operated Mobile Service Operations. For information related to Mobile Servicing, see the "July 2021 Mobile Service Guidebook" published in GlobalConnect (GCUS-9-11572).

B. GENERAL NOTES

The infrastructure guidelines are organized as follows:

- **Operating Minimum** – The minimum acceptable systems infrastructure capability/components for conducting business with GM*
- **Operating Recommended** – 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 "Operating Recommended" section.

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 Microsoft Surface Pro 9 Non-branded, built by hand or thin client PC
Intel Core i3 / i5 / i7 / i9 processors 7th generation and above	ALL Intel Core i-series 6th generation and below Processors plus AMD, Celeron, Pentium, and Atom processors
Windows 10 & 11 Professional, 64-bit Windows Server 2016 Standard	All Operating Systems **except** Windows 10 & 11 Professional, 64 bit and Windows Server 2016 Standard All Home Operating Systems Tablets running Android or Mac operating systems
Java Run Time Environment 32 bit	All 64-bit versions of Java

DESKTOP PC, LAPTOP, & TABLET PC'S

	Operating Minimum*	Operating Recommended
Processor	Intel Core i3, i5, i7 7th Gen	Intel Core i5, i7, i9 8th Gen* & above
System memory (RAM)	16 GB +	16 GB +
Hard Disk Drive (HDD or SSD)	500 GB +*	1 TB +
CD / DVD Drive (Optional)	CD/DVD Combo or external drive	CD/DVD Combo or external drive
USB A 2.0 & 3.0+	2+	2+
USB C 3.1+	1+	2+
Network Adapter	Wired: Gigabit Wireless: 802.11ac	Wired: Gigabit+ Wireless: 802.11ax
Operating System	Windows 10 & 11 Professional, 64-bit	PC: Windows 10 & 11 Professional, 64-bit or Windows Server 2016 Standard (EPC)

Note (Processor): 8th Generation or above have model numbers of 8000 or greater (i.e.: Intel Core i5-8500).

*Note (Hard Disk): When using for EPC (Electronic Parts Catalog) the Free Disk Space requirement to support a local EPC installation can exceed 500 GBs. 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.*

Note (Remote Connection Services): 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.

Note (Operating Minimum): Hardware that doesn't meet the "Operating Recommended" specifications may not be supported by Snap-on upon contract renewal.

Note: 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.

For the Techline Service Technician applications (Techline Connect, 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.vii 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 or USA – 19HS – C) for computers without serial ports
- Recommended Service Programming USB standard
    - FAT 32 – File Allocation 4096 (64KB)
    - Size 16 or 32 GB USB 2.0

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.

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.

	Operating Minimum	Operating Recommended
Word Processing	Microsoft Word Mobile	Office 365 ProPlus
Spreadsheets	Microsoft Excel Mobile	Office 365 ProPlus
Presentation	Microsoft PowerPoint Mobile	Office 365 ProPlus
Endpoint Protection	An endpoint detection and response (EDR) solution should be deployed on all computers/servers.	An endpoint detection and response (EDR) solution should be deployed on all computers/servers.
Web Browser*	Microsoft Edge version 92+, Google Chrome version 93+	
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.	
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)

Note (Web Browser): Global Warranty Management supports the use of EDGE. Chrome is not supported.

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)

	Operating Minimum	Operating Recommended
Local Area Network	Ethernet based 1 Gigabit	Ethernet based 1 Gigabit
Data Cabling*	Cat-6a+	Fiber optic cable
Equipment Location	Locked room	Locked, clean, and temperature-controlled room
	LAN wiring should terminate & equipment should be housed in a wiring closet or communications room	
IP Addressing*	Dynamic addressing (DHCP)	
Network Adapter	1 Gigabit	1 Gigabit
Traffic Switching	1 Gigabit Managed switch	1 Gigabit Managed switch
Routers/Access Points*	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.	
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.)	
Ethernet Standard Specification	IEEE 802.3ab 1000base-T	IEEE 802.3.an 10Gbase-SX+
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	1000+ Mbps	2+ Gbps
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 IEEE 802.11ac	Dual Band IEEE 802.11ax or better
Network Documentation	Labeled cables & Pictures of IT equipment from front and back stored locally and in a cloud accessible location. ISP contract information stored locally and in a cloud accessible location.	Labeled cables & Pictures of IT equipment from front and back stored in a cloud accessible location. ISP contract information stored locally and in a cloud accessible location. Network drawings completed in network diagram software depicting models, IP addresses, IP Addresses, Routing protocols, OS versions

Note (Data Cabling): Fiber optic cable is necessary in place of data cable runs when the length exceeds 328 feet (100 meters).

Note (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.

Note (Routers/Access Points): 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.

II. WI-FI

	Operating Minimum	Operating Recommended
Network Standard	802.11ac with RADIUS authentication	802.11ax with RADIUS authentication
Authentication & Encryption*	WPA2 Enterprise with RADIUS authentication and AES Encryption	WPA2/WPA3 Enterprise with RADIUS authentication and AES Encryption
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. An access point must be within 120 feet (37 meters) of all coverage points. Access points within the sales showroom, service drive, service shop, and customer lounge should be within line-of-sight.	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. An access point must be within 120 feet (37 meters) of all coverage points. Access points within the sales showroom, service drive, service shop, and customer lounge should be within line-of-sight.
Wireless Hardware*	A wireless LAN controller can be used in combination with the Lightweight Access Point Protocol or Control and Provisioning of Wireless Access Points protocol (LWAPP or CAPWAP) to manage lightweight access points across the dealership network. 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	Dealers must ensure guest traffic, financial data, and the dealership network are segmented 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.	
Wireless Threat Detection	Continuously scan, identify, and remove any wireless threats that may be on the dealership's network.	
Customer/Guest Access	Dealerships should utilize a firewall or other mechanism to limit guest bandwidth consumption and illegal file sharing. This will prevent guest access from interfering with business operations by consuming too much bandwidth. Additionally, guest network wireless access is configured to be separate from production network and access passwords are changed every 90 days.	

	GM encourages dealers to 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. Additionally, GM encourages that the guest network be disabled after business hours.
Network Mobility	Utilize a wireless mesh network to ensure end users can navigate around the location without losing connection or authenticating again.
Channel Configuration	Access points will be configured to use the following channels: • For 2.4 GHz… Channels 1, 6, or 11 ONLY. • For 5 GHz… Channels 36-64, 100-140, or 149-165.
Network Monitoring	Monitor and report on all connected devices, bandwidth utilization, signal strength, segmentation, and security activity.

Note (Authentication & Encryption): WPA2/WPA3 should not be confused with WPA3 standalone. Not all GM tools and equipment currently support WPA3.

Note (Wireless Hardware): 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.

Service Department Notes:

- *WPA2 authentication is required for Service Advisor Vehicle Interface (SAVI) to function. SAVI is available to United States Dealerships only.*
- *SAVI requires an access point within 120 feet (37 meters) of every point within the service lane if using 2.4Ghz frequency band and 65 feet (20 meters) if using 5Ghz. Access points should within line-of-sight.*
- *The MDI, MDI 2, and SAVI tools do not support RADIUS authentication; however, it is still possible to implement WPA2 Enterprise 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, MDI 2, and SAVI are not compatible with an open, unencrypted wireless network.*

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. Additionally, GM labor times for vehicle firmware and software downloads assume a minimum speed of 40 Mbps for each active event. It is critical that the dealership procures enough bandwidth to adequately provide enough bandwidth so that employees and customers can quickly access data.

Dealer Network Size	Operating Minimum	Operating Recommended
Small **(1 - 30 Endpoints)**	Sales Showroom: 15 + Mbps Guest Lounge: 10 + Mbps Service Drive: 15 + Mbps Service Garage: 45 + Mbps *Administration/Other: 15 + Mbps Vehicle Lot: 10 + Mbps *Total (Up/Down): 100 + Mbps*	Dynamically balance bandwidth based on active data requests through redundant ISP Connections. Business groups should be prioritized in the following order, if applicable: 1. Service Garage 2. Sales Showroom 3. Service Drive 4. Administration/Other 5. Guest Lounge & Vehicle Lot *Total (Up/Down): 200 + Mbps*
Medium **(31 - 80 Endpoints)**	Sales Showroom: 30 + Mbps Guest Lounge: 15 + Mbps Service Drive: 25 + Mbps Service Garage: 90 + Mbps *Administration/Other: 30 + Mbps Vehicle Lot: 10 + Mbps *Total (Up/Down): 200 + Mbps*	Dynamically balance bandwidth based on active data requests through redundant ISP Connections. Business groups should be prioritized in the following order, if applicable: 1. Service Garage 2. Sales Showroom 3. Service Drive 4. Administration/Other 5. Guest Lounge & Vehicle Lot *Total (Up/Down): 300 + Mbps*
Large **(81+ Endpoints)**	Sales Showroom: 45 + Mbps Guest Lounge: 20 + Mbps Service Drive: 35 + Mbps Service Garage: 140 + Mbps *Administration/Other: 45 + Mbps Vehicle Lot: 15 + Mbps *Total (Up/Down): 300 + Mbps*	Dynamically balance bandwidth based on active data requests through redundant ISP Connections. Business groups should be prioritized in the following order, if applicable: 1. Service Garage 2. Sales Showroom 3. Service Drive 4. Administration/Other 5. Guest Lounge & Vehicle Lot *Total (Up/Down): 1 + Gbps*

Note (Administration/Other): Administration/Other consists of business groups such as: finance and purchasing, information technology, supply chain, etc.

Note: Dealerships can both allocate and limit bandwidth through modern gateways/access point configuration settings.

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. It is recommended the backup internet connection should be at least the same speed as primary connection if possible 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 following security guidelines represent the **minimum** set of security capabilities that should be in place, and properly functioning, to reasonably protect information and ensure that it is safe from loss, theft, unauthorized access, copying, modification, use or disclosure during utilization, transmission and storage. Each dealership has the responsibility to protect confidential information. For purposes of these guidelines, confidential information is defined as dealer information and data that should not be accessible to anyone without a "need to know". Each dealership must ensure the security of customer information, including confidential information held on behalf of customers or clients.

Protecting dealership data means protecting its confidentiality, integrity, and availability. The potential consequences of a failure to protect all three of these aspects include business losses, legal liability, and loss of company goodwill. Although this document is intended to provide guidance, tools, and assistance to aid dealerships in securing dealer data, dealer data security is the responsibility of the dealership. Dealer service providers, third parties, and General Motors cannot guarantee a secure dealer network, even if dealers follow the guidelines in this document. GM also recommends that dealerships turn to industry experts, industry and federal guidelines, and other knowledgeable resources for help with dealer data security. Additional guidelines for dealership security include security documentation published by the National Institute of Standards and Technology (NIST), Standards of Technology in Automotive Retail (STAR), SANS.org, ISO 27001, ISO 27002 and cisa.gov/shields-up .

Note: Perform annual audits and assessments of all of the below requirements (Sections I – VI). The Dealer Principal must receive annual audit and assessment results and be informed of all mitigation/action plans.

I. INFORMATION SECURITY GOVERNANCE & IDENTITY ACCESS MANAGEMENT

To enforce adequate information security, policies must be defined and implemented to address business strategy, regulations, legislations, and contracts as well as the current security threat environment.

A security policy typically consists of several individual security policies. The section that follows provides recommendations and advice for policies commonly found within an organization's security policy.

Management	Assign designated roles and responsibilities for security within the organization and network (e.g., CISO or Cyber Manager, guest, administrator, user, etc.) and create rules and procedures to clearly delineate between different roles and responsibilities
Asset Management	Develop and maintain guidelines for identifying, registering, and managing assets throughout their lifecycles to remain current with all relevant assets and their owners, (e.g., asset inventory, leased inventory).
Compliance	Dealer maintains self-assessment processes to ensure compliance to these security requirements and provides proof of compliance upon request.
Training	Conduct annual training and awareness campaigns on information security.
Administration	Publish and maintain an official Information Security Policy, and related standards, guidelines, and procedures, for employees, and external parties (e.g. customers, affiliates, suppliers, partners, etc.). This should include a policy for limiting information access to employees based on their "need to know".
Access Rights Policy	A policy is defined and documented which limits access to information by employees based on their "need to know". All accounts and access rights must be reviewed at least semi-annually to determine if access is appropriate based on business need. Evidence of this review must be retained for a minimum of one year. A process must also exist to remove accounts and access rights immediately after employment termination.
Acceptable Use Policy	An acceptable use policy for digital devices, internet, and applications is defined and documented and includes: • Restricting employees and customers from accessing inappropriate sites on the internet • Using dealership assets for personal use • Restrict employees to downloading only files or applications with business justification • Restrict customers from downloading any files or applications • All employees sign a computer use policy prior to accessing dealership systems, applications, and customer information
Incident Response Policy	A step-by-step process exists to respond, resolve, and recover from a security incident. Testing and validation of this incident response processes should occur annually.
Retention Policy	A retention policy exists and is used to manage physical and electronic records which contain customer information or confidential information.
Data Back-Up Policy	A process exists for backing up business critical information and restoring information within 1 day in the event the information is lost or compromised.
Social Engineering Policy	A process exists to protect against, and report attempted social engineering. For example: • Ensure caller identity is validated before granting access to any information. • Report any suspect engagements trying to obtain information or connect to resources at the dealership.

	• Ensure the following is never shared over the phone with someone who calls the dealership: -passwords -social security numbers or other government identifiers -credit card numbers or loan identifiers
Security Policy Communication	Employees acknowledge review of policies and attest to compliance. Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

II. ACCOUNTS, ACCESS, PASSWORDS, & LOGINS

Account/Access Rights	• All accounts (including service accounts) and access rights are reviewed at least semi-annually to determine if access is appropriate based on job function. • Each user account is assigned to and used by only one individual. • Ensure all devices that contain or can access customer information or confidential information require password access. • All passwords (i.e., servers, firewalls, routers, IDS, software, etc.) are changed from their default values. • Access rights are immediately removed from employees who no longer work for the Dealer.
Account Credential Management	Usernames and password policies are managed by a centralized directory service (e.g. Active Directory).
Account Configuration	Computer system service accounts are configured to only allow already logged in users to log in. (i.e., switch user command).
Password Requirements	Passwords must be changed at least every 90 days and controls exist that forces users to comply with password policy requirements. • Passphrases are used instead of passwords with at least 12 characters that include a combination of upper and lowercase letters and numbers. • Users are not able to reuse their last five (5) passwords. • Remove employee credentials from all network devices immediately upon employment ending.
Login Requirements	• User accounts are locked-out or suspended after the tenth (10) failed sign-on attempt. • Ensure user's identity is verified before resetting their password. • If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
Multi-factor Authentication	Implement Multi-Factor Authentication (MFA) anywhere possible. MFA is critical to stopping threat actors from using mass data leaks to gain access to otherwise secure systems.

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

Firewall/ Unified	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.

Threat Management (UTM)	The device should also have the following features: • 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 Procure backup Firewall/UTM appliance. Install in high availability configuration for auto failover in the case of primary device failure.
Network Segmentation	Payment Card information, customer information, dealership traffic, and customer traffic must 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 category Content Filtering
Network Access Points	Remove/disable unnecessary network ports, protocols, and access points whenever applicable.

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

IV. DATA SECURITY

Security Information Event Management (SIEM)*	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.
Penetration Testing and 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
Email Security	• 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
OS/Software Maintenance	Ensure all versions of operating systems and application software are current, and that security patches are regularly applied.
Data Transfer	Use secured methods to transfer structured and unstructured data.
Removable Media	Prohibit the use of removable media (e.g., USB, external hard drives, etc.) when possible.
Cached Data	For walkup kiosks, and other public digital interfaces, cached data should be cleared after 5 minutes of inactivity.
PC Virus Monitoring	An endpoint detection and response (EDR) solution should be deployed on all computers/servers 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 solution should be a combination of data collection, data analysis, forensics, and threat hunting, with the end goal of finding and blocking any potential security breaches as well as: • 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

Note (SIEM): Reactive management software (i.e. Desktop firewall or antivirus, Remote Management Software) 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.

Note (SIEM): Reactive 24x7x365 security event monitoring and response should include not only around the clock alerting, but immediate response to potential threats.

V. DISASTER RECOVERY & BUSINESS CONTINUITY

Disasters can come in many forms. A disaster could be caused by power outage, tornado, fire, flood, construction that cuts network communication, hacker event, etc.

Adequate plans must be put in place to prepare for, mitigate and respond to a disruptive event, ensuring that personnel with the necessary authority, experience and knowledgebase are in place.

Data Recovery	Network gateway configuration and critical data should be backed up and maintained in the case of network or hardware failures. Publish and maintain an official Data Recovery Policy, and related standards, guidelines, and procedures, for employees, and external parties (e.g. customers, affiliates, suppliers, partners, etc.). Annually test and audit data recovery processes, standards, and procedures.
Onsite Risk Mitigation	Uninterruptible Power Supplies (UPS) are used for all business-critical equipment.

VI. PHYSICAL SECURITY

Physical security prevents unauthorized physical access to secured areas or data (paper or electronic). Procedures and controls must be established to ensure sensitive or critical data is protected.

Dealership Surveillance	Dealership facility is under constant surveillance (including any computer devices and networking/computer closets).
IDF Closet / Server Room	Network / computer closet is physically locked, and access is limited to IT personnel.
Equipment & Kiosks	Desktops and kiosks are locked in a physical enclosure with no exposed ports. Unattended devices that contain confidential or customer information are locked or permanently affixed to the building or desk that it rests upon (e.g., laptops, desktops, storage devices, etc.
Physical Access Controls	Implement and monitor physical access controls at ingress/egress points, where possible (e.g., door locks, alarms, badge readers, surveillance cameras, etc.).

VII. TECHLINE AND SERVICE ADVISOR VEHICLE INTERFACE APPLICATION SECURITY, FIREWALL EXCEPTIONS

All application updates and installations must be performed from an account with local Windows administrative privileges. Firewall Exceptions for 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)\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)\Vibe Programming\Cuw.exe
- Firewall Exceptions:
  - galileo-api.ext.gm.com
  - gsitlc.ext.gm.com
  - tlc.gm.com
  - sps.gm.com
  - techline.gm-cdn.com
  - gspas-delivery.gm-cdn.com
  - sps-info.gm.com
- Service Advisor Vehicle Interface (SAVI) firewall exceptions:
  - gmdealerservices.gm.com (Port: 443)
  - api.bitbrew.com (Port: 443)
  - ota.bitbew.com (Port: 443)
  - apim.gm.com (Port: 443)
  - portal.bitbtrew.com (Port: 443)
  - tla.ext.gm.com (Port: 8883 & 7000)
  - time.google.com
  - time1.google.com

- time2.google.com
- time3.google.com
- time4.google.com

3. GLOSSARY OF TERMS

Administrator – A person who manages the technical aspects of a system.

Authentication – The act of establishing or confirming the identification credentials of a person or system.

Availability – Ensures that information is accessible when and where it is needed.

Confidentiality – Ensures that information is not disclosed to anyone who is not authorized.

Encryption – The conversion of digital information into a format unreadable to anyone except those possessing a "key" through which the encrypted information is converted back into its original form (decryption), making it readable again.

Firewall – Software or hardware that, after checking information coming into a computer from the Internet or an external network, either blocks the transmission or allows it to pass through, depending on the pre-set firewall settings, preventing access by hackers and malicious software; often offered through computer operating systems.

Integrity – Ensures that information is correct or accurate to the degree anticipated by those who use it. It also ensures that information has not been changed and has not been exposed to unauthorized modification.

Intrusion Detection Systems (IDS) – Hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)

Intrusion Prevention System(s) (IPS) – System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

IP Address – A unique identifier in the form of a numerical label assigned to each device, such as a personal computer or server, participating in a network, such as the Internet.

Local Area Network (LAN) – A computer network that links devices within a building or group of adjacent buildings. A "local" network.

Malware – Short for malicious software. Software that disrupts or damages a computer's operation, gathers sensitive or private information, or gains access to private computer systems. Malware may include botnets, viruses, worms, Trojans, keyloggers, spyware, adware, and rootkits.

• Botnet – a network of private computers, each of which is called a "bot," infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes.

• Virus – has a reproductive capacity to transfer itself from one computer to another spreading infections between online devices.

• Worm – replicates itself over and over within a computer.

• Trojan – gives an unauthorized user access to a computer.

• Spyware – quietly sends information about a user's browsing and computing habits back to a server that gathers and saves data.

• Adware – malware that allows popup ads on a computer system, ultimately taking over a user's Internet browsing.

• Rootkit – opens a permanent "back door" into a computer system; once installed, a rootkit will allow more and more viruses to infect a computer as various hackers find the vulnerable computer exposed and attack.

Modem – An electronic device that converts a computer's digital signals into specific frequencies to travel over telephone or cable television lines; computers use modems to communicate with one another over a network; often used to link home computers to the internet through an internet service provider.

Network – A collection of computers interconnected by communication channels that allow sharing of resources (hardware, data, and software) and information.

Patch – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Penetration Testing – A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system

Phishing – Sending emails that attempt to fraudulently acquire personal information, such as usernames, passwords, social security numbers, and credit card numbers, by masquerading as a trustworthy entity, such as a popular social website, financial site, or online payment processor; often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Pop-ups – A form of online advertising on the worldwide web intended to attract web traffic or capture email addresses; created by advertisers, pop-ups generally appear unexpectedly in a small web browser window when a user is linking to a new Web site.

Security Incident – A breach or imminent breach of IT security defenses that may have a negative impact. These impacts may include, but are not limited to; fraudulent activity, unauthorized disclosure, unauthorized modification, identified vulnerabilities and intrusions or incidents of impaired or denied availability to the computing and communications environment.

Server – A computer program or physical computer that services other computers over a local network or the Internet; network servers typically are configured with additional processing, memory, and storage capacity; specific to the Web, a Web server is a computer program (housed in a computer) that serves requested HTML pages or files.

Service Account – Accounts used by systems or applications to interact with other applications or the operating system, run batch jobs or scripts, or provide access to other applications. For the purpose of this policy, accounts that can be used interactively are considered user accounts and not Service Accounts.

Social Engineering – An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Spam – The use of electronic messaging systems to send unsolicited bulk messages (usually advertising or other irrelevant posts) to large lists of email addresses indiscriminately.

Spyware – A type of malware (malicious software) installed on computers that collects information about users without their knowledge; can collect Internet surfing habits, user logins and passwords, bank or credit account information, and other data entered into a computer; often difficult to remove, it can also change a computer's configuration resulting in slow Internet connection speeds, a surge in pop-up advertisements, and un-authorized changes in browser settings or functionality of other software.

TLS (Transport Layer Security) – Cryptographic protocols that provides communication security over the Interne

USB (Universal Serial Bus) Flash Drive – A data storage device that is typically removable (plugged into a USB/Universal Serial Bus port on a personal computer) and rewritable, and physically much smaller than a floppy disk.

USB (Universal Serial Bus) Port – A single, standardized way to connect devices (modems, printers, scanners, digital cameras, etc.) to a personal computer.

User Accounts – All user and administrative accounts used for interactive logons (i.e., user ID and passwords).

Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Wi-Fi – Technology that allows an electronic device (personal computer, video game console, smartphone, tablet, digital audio player) to exchange data wirelessly (using radio waves) over a computer network.