STAR®

Standards for Technology in Automotive Retail

STAR Dealer Infrastructure Guidelines

2016

INDUSTRY BEST PRACTICES AND RECOMMENDATIONS FOR AUTOMOTIVE RETAIL INFORMATION TECHNOLOGY

1. STAR Dealer Infrastructure Guidelines

1.1 Overview

This comprehensive document – STAR Dealer Infrastructure Guidelines (DIG) - outlines the industry best practices and is to be referenced by dealers to verify network and infrastructure needs. Dealers small and large should have internal network administrators - or IT Managers - who are responsible for reviewing these guidelines, checklists and tips along with its Quick Reference Guide to ensure their dealership has implemented a safe, secure and robust solution which meets both the customer and dealership team's needs.

1.2 The DIG Workgroup (WG)

The Dealer Infrastructure Guidelines (DIG) is supported by one of the several Workgroups (WG) within the STAR organization. Unlike many of the WGs which are charted to focus on data structures and transports, the DIG was established to assist dealers, vendors, and OEMs with a common guidebook for the needed IT infrastructure to support a secure, efficient and robust automotive dealership.

1.3 DIG Benefits – Dealer, Vendor, and OEM

Similar to other retailers, the automotive dealership needs to have the right technology to support robust processes aimed at selling and servicing vehicles. With the advent of the internet, many different systems are leveraged within a dealership to meet the ever-growing demands of the customers. These dealer systems are provided and support by Dealer System Providers (DSP) and include everything from the core Dealership Management System (DMS) to numerous supporting solutions such as Customer Relationship Marketing (CRM), Lead Management, Equity Mining, Reputation Management, Websites, Digital Marketing, Online Inventory Management, Service Lane Tools and many others. With the ever-growing need for DSPs, there is also a need for data to be efficiently and securely shared between these dealer systems and OEMs. This DIG is intended as a guide to support effective data integration, data protection, system reliability and efficient business processes.

1.4 Disclaimer

Any company name, application, website link, or technology reference mentioned in this document should not be considered an endorsement by the OEMs or by STAR unless that endorsement is expressly stated.

This document provides a basic specification or guideline for dealers to establish Internet communication. It is important to note that network infrastructure, dealer data, and system security is the dealership's responsibility. Third-party organizations such as service providers and partners may provide guidance and recommendations. Some organizations may provide software, hardware, or proprietary network elements to help streamline network operations. However, these applications, recommendations, or tools are not a substitute for network management.

2. Dealer Network Infrastructure

2.1 Overview

A dealership's network infrastructure consists of the 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 users, service providers, the OEM, and end customers. Proper selection and implementation of network infrastructure are critical to ensuring network efficiency and compatibility with OEM, DSP, and dealership applications and data.

2.2 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 very expensive capital expenditure, old hardware can 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.

2.2.a When to Purchase New Hardware?

Well-maintained IT hardware may last three to five years or even longer, in some cases. However, at some point a dealer will need to weigh the options of upgrading - or replacing - current hardware.

STAR recommends that dealerships consider replacing hardware in the following situations:

- When the current hardware does not meet minimum specifications needed to operate a specific technology.
- Current hardware falls below minimum standards set by an OEM, DSP or other dealership technology partner.
- Does not have the hardware, accessories, or support the peripherals need for a specific function.
- The device performs so slowly it affects business operations. *Please note*: *This may not necessarily be due to a hardware issue. Slowness can be due to configuration, storage, security, or user error.*
- New software (such as operating systems, browsers, or dealer applications) is not compatible with current hardware.
- New hardware could provide enough cost savings due to time savings, added features, or ease of use.
- Upgrade costs are at or near the cost of a replacement, or the product is nearing end-of-life and/or is no longer supported.

2.2.b What to Purchase: Consumer-grade vs. Enterprise-grade Hardware

Most computer manufacturers 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.

STAR recommends dealerships purchase enterprise-grade hardware for the following reasons:

- Consumer-grade systems are typically made with more generic parts or parts that are less costly to supply in bulk. Also, the manufacturers are known to switch parts, suppliers, and components without changing up the models. Because of these factors, these parts may have a higher failure rate. This can lead to more downtime, longer support time, and slower system replacement turnaround rate.
- Enterprise-grade systems are typically made with standardized, name brand parts, making network standardization and support easier for many businesses.
- Consumer-grade PCs often come with operating systems intended for home use. This can result in business networking challenges like connecting to servers or other PCs.
- Consumer-grade networking hardware is often intended only for a small number of connections. Enterprise-grade hardware is designed to accommodate the large number of connections dealership networks require.
- Consumer-grade hardware may come with limited warranties. Some consumer warranties do not extend to businesses.
- Initial savings could be offset by costlier replacement and tech support as well as longer turnaround times to secure a replacement.

2.2.c Hardware Recommendations

Desktop PCs	
Component	**Specifications**
Processor	Intel Core i5 and above, or AMD equivalent
Memory (RAM)	4 GB or more
Hard Disk Drive	500 GB or more
CD/DVD Drive	CD/DVD combo
Serial Port	1 (Optional USB adapter)
USB Ports	2 or more
Audio Adapter	16 bit
Audio Speaker	Optional
Display	1280x768 minimum resolution
Network Adapter	Wired: Gigabit (or greater) Ethernet Wireless: 802.11 n
Warranty	3 year on site
Operating System	Windows Operating Systems are compatible with most dealership applications. Please see your OEM and technology partners when choosing an operating system.

Laptops	
Component	**Specifications**
Processor	Intel Core i5 and above, or AMD equivalent
Memory (RAM)	4 GB or More
Hard Disk Drive	320 GB or more
CD/ DVD Drive	CD/DVD combo
USB Ports	2
Audio Speaker	Optional
Display	1280x768 minimum resolution
Network Adapter	Wired: Gigabit (or greater) Ethernet Wireless: 802.11 n
Warranty	3 year on site
Operating System	Windows Operating Systems are compatible with most dealership applications. Please see your OEM and technology partners when choosing an operating system.

Routers & Switches	
Component	**Specifications**
Ethernet Standard Specification	IEEE 802.3 100baseT or 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 or 1000 Mbps
VLAN	Switches with VLAN and 802.1Q trunk technology should be used for routed networks with multiple subnets or VLANs.
Management Protocols	Managed devices should support industry remote management standards such as Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).
Wireless Switches	Wireless devices should be dual band and IEEE 802.11b/g/n compatible.

2.2.d 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 higher mobility and accessibility.

Some applications are specifically developed to run on certain tablet devices such as iPads. When these applications are deployed, the OEM will communicate with 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 versions.

2.2.e Decommissioning & Recycling Hardware

It is the original device owner's responsibility to ensure all used electronics are disposed of properly. There are thousands of electronic recyclers in the US, but it is important to choose the right one. Below are some suggestions to follow when choosing a recycler.

Find out the recycler's policies / practices for destroying personal data on used equipment.

- Data can be wiped from storage media using a magnetic wiping method or a program to overwrite all sectors of a hard drive. Any method used for data wiping should be done more than once (multi-pass).
- Storage media can be destroyed by shredding, cutting, incinerating, multiple perforations or crushing.
- A recycler should be able to provide written certification that the data was wiped- or storage media destroyed- as well as provide a record of the method(s) used.

Find out the recycling company's certification(s).

- The recycler should be certified. If told they are not certified, it is a 'trade secret' or that their method is 'confidential', avoid using them.
- The main industry certifications are:
    - E-Stewards – www.e-stewards.org
    - Basel Action Network – www.ban.org
    - R2 – www.sustainableectronics.org
- Recyclers and consolidators should be able to produce evidence that they have the proper facilities, training, and equipment to perform the claimed operations by showing an audited management/operations system complete with evidence of recent audits.
- Ask if the recycling company has an environmental management certification or system in place; either an ISO 14001 environmental management certification or certifications by organizations like the International Association of Electronics Recyclers (IAER) or the Institute of Scrap Recycling Industries (ISRI).
- For those that are not certified, caution is advised. The dealership, as the original device owner, has the responsibility to ensure proper recycling.

Find out if the recycler has had any environmental or safety violations (citations, fines, notice of violation, consent orders, etc.) or have filed for any environmental damage insurance claims in the last 5 years.

- Companies that have a good track record of complying with environmental and safety requirements are preferred.
- A company that has been in business for several years with only a few minor violations that were quickly resolved may be just as responsible as a company with only a year or two in the business with no violations.
- Check for major violations such as large quantity waste releases or significant neighborhood complaints.

Find out if the recycler sends used equipment or wastes to other business partners or service providers; these are called 'downstream partners'.

- Good recordkeeping is an industry best management practice. Look for companies that keep detailed records including where they ship materials, how much they ship and serial numbers for items to be reused.
- Although there are several "full service" recyclers in the U.S., it is likely that the recycler will not handle the full processing of the device.

- The recycling company should have written logs of what processing is done on site (such as sorting and/or shredding) and who receives the materials or products after the initial processing.
- Ask if the recycler's business partners (Downstream Partners) are contractually bound to the same standards or best management practices as the chosen recycler. A complete listing of all downstream partners should be available from the chosen recycler.
- Be wary of recyclers who state that their processes and business partners are "confidential," "proprietary," or that "they don't know."
- All exporting must be done in compliance with laws applicable to both the exporting and importing countries.

A recycler should have general liability and environmental liability insurance.

- Insurance requirements vary from state to state, and the amount and type of coverage necessary will vary by the size and operations at the facility.
- The amount and coverage will depend on the scope and magnitude of the operations.

2.3 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.

For dealerships, these programs or processes often reside on a PC's operating system or internet browser. Software is often designed for specific operating systems or internet browsers. Because software is critical for dealer communications and business processes, it is important dealerships utilize operating systems and browsers that are compatible with dealership software.

The following section details common operating systems and browsers. The goal of this section is to provide guidance for understanding and selecting operating systems and browser applications. It is strongly recommended the dealer check with their OEM and dealership service providers to ensure software compatibility with dealerships applications.

2.3.a Operating Systems

Below is a list of the most common operating systems in the market today. Some applications are not compatible with specific operating systems. It is recommended that dealers check with their OEMs, DSPs, and other vendors to determine which operating systems to use. Please note, as of April of 2014, Microsoft ended support for XP operating systems. This includes critical security updates. STAR recommends dealerships do not use Windows XP.

Current Common Client Operating Systems	Latest update or service pack*	End of mainstream support	End of extended support
Windows XP	Service Pack 3	14-Apr-09	8-Apr-14
Windows Vista	Service Pack 2	10-Apr-12	11-Apr-17
Windows 7	Service Pack 1	13-Jan-15	14-Jan-20
Windows 8	Windows 8.1	9-Jan-18	10-Jan-23
Windows 10, released in July 2015	N/A	13-Oct-20	14-Oct-25
MAC OS X	10.9 (or higher supported) 10.11	Versions 10.8 (Mountain Lion) and below no longer supported.	Versions 10.8 (Mountain Lion) and below no longer supported.
IOS (for iPad and iPhone)	9.1		
Android	5		

Latest updates/service pack as of November 2015

2.3.b Internet Browsers

Below is a list of the most common internet browsers in the market today. Some applications are not compatible with specific browsers. Other applications require specific browser settings, such as compatibility mode. It is recommended that dealers check with their OEMs, DSPs, and other vendors to determine which operating systems to use.

Browser	Latest update or service pack*	Notes
Google Chrome	46	
Mozilla Firefox	41	
Internet Explorer	11	
Apple Safari	9	Not recommended for use on Microsoft Operating systems
Opera	32	

Latest updates/service pack as of November 2015

2.3.c Software Licensing

Software licensing compliance is something on which most dealerships may not be focused. However, it can cost a dealership thousands of dollars if ignored. Here are the most common mistakes in software licensing for a dealership.

- Sharing a common license instead of having one per device.
- Sharing logins for cloud-based software.
- Having legally licensed copies of software installed but not used.
- Buying “home” versions of software instead of business or enterprise class.
- Using pirated software, downloaded for free.

To address this problem, companies need to create a Software Asset Management (SAM) program. SAM is the practice of managing and optimizing the purchase, deployment, maintenance, and lifecycle of software assets within an organization. The two biggest benefits of a SAM program are cost control and risk reduction.

2.4 Local Area Network (LAN)

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 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.

2.4.a Network Configuration & Management

Recommendation	Specification
Local Area Network	Gigabit Ethernet
Data Cabling	Existing data network cabling should be - at a minimum - TIA-568-A Category 5e standards. Category 6a should be used for new cabling. No horizontal cable runs should exceed 90 meters (295 feet). Fiber optic cable is highly recommended in place of data cable runs when the length exceeds 295 feet.
Equipment Location	LAN equipment should be housed in a wiring closet or communications room. All equipment should be mounted or secured to a rack or shelf.
IP Addressing	Dealership ISP should provide routable IP addressing. For the dealer LAN, dynamic addressing (DHCP) should be used to ease support.
Network Adapter	Gigabit Ethernet
Ethernet Switching	Gigabit Managed Switch. Label each interface and cable. This will save time when tracking back network cables for support or new installation.
Routers	Business-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.
Firewall	A 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, antivirus, and stateful packet inspection. - Firewalls should support Network Address Translation/Process Analytical Technology (NAT/PAT). Firewalls 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. - For more information on firewalls and network security see section 2.6.
Domain Name Services (DNS)	Use public DNS except when using Windows Active Directory. (In which case, having an internal DNS server is required.)

2.4.b Wireless Networking

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.

Use the following guidelines when designing, supporting, and securing a dealership wireless network.

Wireless Networking Design

Recommendation	Specification
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. Business 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.
Coverage	Deploy wireless access points to ensure adequate coverage. Wireless tools can provide signal strength around the building. Be aware of structures or objects that can interfere with wireless coverage (electrical interference, radio frequency interference, or physical materials such as metals or concrete).
Authentication & Encryption	WPA2 with RADIUS authentication and AES Encryption
Network standard	802.11n or 802.11ac
Rogue Wireless Detection	Scan, identify and remove any rogue wireless access points that may be on the dealership's network. -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, IT management, and ownership. -All rogue wireless networks must be detected, found, and removed immediately. -STAR recommends the use of a managed wireless detection service that is continuously scanning the network for wireless threats.

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	STAR 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.
Internet Bandwidth	To ensure the dealership has enough bandwidth, a dealer must choose the right technology and speed. (See Section 2.5a and 2.5b in the STAR DIG for more information on technologies and internet bandwidth.) -STAR also recommends every dealership have a backup ISP connection from a different provider, using a different technology. -See section 2.5c for recommendations on internet backup connections.

2.5 Internet 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.

The following section details the technologies available for internet access and how to plan for enough bandwidth for each resource on the local area network (LAN).

2.5.a Internet Technologies

Technology	Description	Speed	Physical Medium	Comments
Cable	Special cable modem and cable line required.	Speeds can vary, but generally runs between 10Mbps and 100 Mbps	Coaxial cable	Cable Internet service utilizes a shared infrastructure and may degrade during heavy usage. Dealerships should look to see what cable providers already have service in the area. The cost of bringing service into an area and trenching cable can be prohibitive. Ford recommends that dealerships purchase business grade cable and ask the provider for a written service level agreement (SLA) or service level objective (SLO)
DSL	Technology uses the unused digital portion of a regular copper telephone line to transmit and receive information. ADSL is asymmetric, meaning the service upload speed is slower than the download speed. SDSL is symmetric, consisting of the same upload and download speeds.	128 Kbps to 52 Mbps	Twisted pair (used as a digital, broadband medium)	Ford recommends dealers purchase business grade DSL lines with enough upload and download speed to run Ford Dealer applications. VDSL is the only recommended DSL - grade as it may be the only service with enough bandwidth to meet the recommended bandwidth requirements.

	VDSL is another asymmetric technology that can offer speeds up to 52Mbps			
T1	Special lines and equipment (DSU/CSU and router) required.	1.544 Mbps	Twisted-pair, coaxial cable, or optical fiber	Multiple T1 lines can be bonded together to achieve greater speeds
Satellite		6 Mbps or more	Airwaves May use dial-up for upstream traffic	Bandwidth is not shared. Also, latency is typically high. This high latency often interferes with dealer applications. Satellite is not a recommended dealer technology.
Fiber	Fiber optic service internet connectivity types operate over an optical network.	As high as 300Mbps	Optical Network	Fiber offers high speeds, lower costs, and good service level agreements. However, availability is limited in some areas of the country.

2.5b Planning for Bandwidth

Start by understanding the current dealership internet service

Many dealerships are unaware of their current internet technology and speed. Understanding the technology can help identify potential limitations and cost savings. Use the chart above to better understand the different technologies available in the marketplace. Find out the current service's bandwidth upload and download speeds (usually identified in Mbps or kbps) by checking with the dealership ISP. Finally, log into the dealership gateway device, ask the dealer ISP, or find tests online to understand current bandwidth utilization.

Plan for spikes in usage

Bandwidth usage is not always consistent. Dealers will see spikes in utilization based upon business processes (such as "busy times"), technology processes (such as running backup or downloading updates), and customer usage (such as streaming video from the customer waiting room). It is recommended that dealerships average around 60% utilization to account for potential spikes.

Plan for technology advancements

Most OEMs, DSPs, and dealership vendors are developing solutions that further leverage internet communications. Dealerships should understand their bandwidth needs are not static, but will continue to grow as the dealership, vendors, and partners implement new technologies.

Plan for Growth

The IEEE (Institute of Electrical and Electronics Engineers) claims that networks will need to be able to support 58% compound annual growth rates in bandwidth. The growth is driven by simultaneous increases in users, access methodologies, access rates and services such as video on demand and social media.

2.5.c Backup Connection

Internet service availability is critical for dealership business. Because dealers rely on the internet to sell and service vehicles, a backup connection is recommended.

When choosing a backup connection, use the following recommendations:

- Use a different provider and internet technology for the backup connection.
- At a minimum have a 3G/4G broadband backup/ failover service available. Test the wireless signal ahead of time to ensure adequate signal strength. Internet service providers, physical location, and building design are variables to signal strength at any given dealership.
- STAR recommends a dedicated circuit for high availability.
- STAR recommends dealerships use a gateway appliance that supports automatic failover to ensure minimal downtime.
- The backup service may not need to be the same speed as the primary connection, but should still have enough bandwidth to support critical dealership business functions.

2.6 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.

The section that follows reviews network protection from the gateway, desktop, security information event management, and data security as well as from the customer and government and risk and compliance standpoints. Further information on security processes and procedures can be found in section 6, titled "Training, Process, and Documentation Practices."

2.6.a Gateway Security (Firewalls & UTM)

Recommendation	Specification
Firewall/ UTM	A fully-managed security device that continually monitors threats through Intrusion Detection system "IDS" and Intrusion Prevention System "IPS" and other mechanisms. 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)
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	Data loss can stem from employees surfing the web for non-business related activities. STAR recommends dealerships filter content on the network to remove potential harmful, inappropriate, or other non-business related traffic.

2.6.b Desktop Security

Recommendation	Specification
PC Virus Monitoring	Enterprise-grade, antivirus 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 • Antivirus solution should include antivirus, anti-spyware, intrusion prevention, application control, spam control and rootkit detection
Patch Management	STAR recommends that patch management 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.
Password Protection	Passwords should be set to expire every 60 days, or less. At a minimum, dealerships should use "strong passwords" containing an 8-character minimum comprised of 3 of the following 4 requirements: 1) Uppercase 2) Lowercase 3) Numeric 4) Special characters.

2.6.c Data Security

Recommendation	Specification
Security Information Event Management (SIEM)	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. *Note: Reactive management software (i.e. Desktop firewall or antivirus) is not to be confused with a proactive SIEM Service.*
Penetration Testing and Vulnerability Scanning	Annual internal and external penetration testing of the dealer network is highly recommended. 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 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. Penetration testing engagements can be performed externally (simulation of an attack from outside of your network and exactly like having a hacking attempt launched from a foreign country), or it may be performed internally (from within your network to see what access and vulnerabilities exist).
Governance, Risk, and Compliance	Comply with all federal, state, local, and industry regulations for financial and retail institutions. PCI Security Standards: https://www.pcisecuritystandards.org Gramm-Leach-Bliley Act: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Certified Integration Partners	Ensure dealer data integrators are certified with DMS and OEM applications. Unauthorized or hostile integration points are often less secure, and sometimes require the dealership to share user and password information.

2.7 Managed Service Providers

Dealers often turn to vendors or partners to help manage, maintain, and secure the dealership infrastructure. A service provider may have the technology or expertise to provide the dealership with a solution to more effectively handle different aspects of the dealer network. Dealers often do not have the time, resources, or expertise to manage an enterprise network alone. Therefore, turning to a service provider could be a logical choice.

A service level agreement (SLA) is very important when selecting a third party to assist with network infrastructure assistance. The provider will make commitments as to what level of service to expect, the scope of service(s), and any refunds or offsetting charges for missed commitments.

The following section provides some guidance in selecting and understanding service level agreements.

2.7.a <u>Service Level Agreements (SLA)</u>

Dealerships receiving IT services are placing a great deal of trust on the Service Level Agreement (SLA) that they select. The SLA will detail the Quality of Service (QoS) that the provider offers with their service – in other words, their guarantee that the service will deliver as promised.

SLAs are used in a wide variety of dealer IT services that include (but are not limited to):

- Internet Service
- Network Integration Services
- Hardware and Software Support Services
- Onsite Support
- Help Desk and Call Center Support

When choosing a service provider, make sure to ask the following questions regarding SLAs.

- Is there a written SLA?
- What are the setbacks, refunds, or other consequences if the provider does not meet their SLA?
- Is there reporting available against the SLA?
- Can the service be cancelled if the SLA is not met?

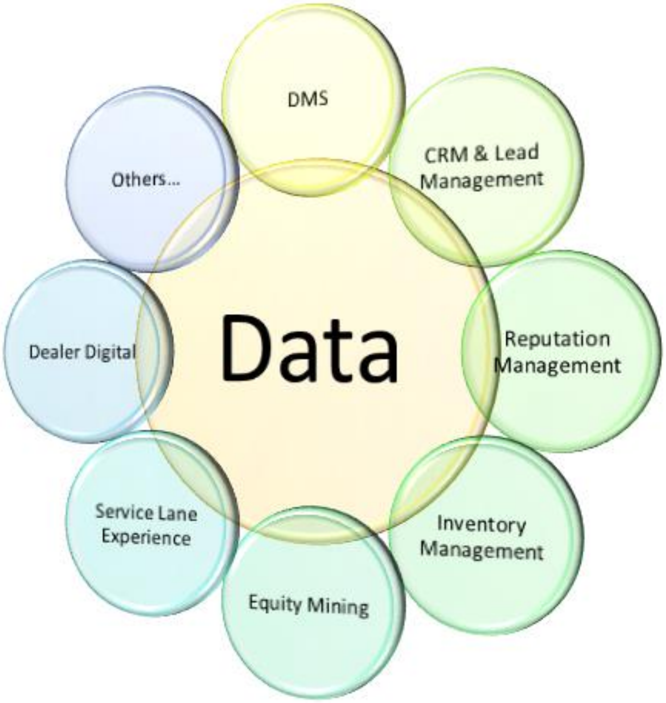
Common SLAs include (but are not limited to):

- Network Availability
- Network Speed
- Network Latency
- Hardware Replacement Time
- Available Support Hours
- Onsite Service Commitments
- Hardware or Software Maintenance Agreements

3. Dealer System Providers

3.1 Overview

The complexity of a dealership and its associated technology has evolved greatly since the inception of STAR. This ever changing technology has continued to enhance the overarching business value of STAR and the integration standards used to align data between systems and processes.



While a Dealer Management System (DMS) has traditionally been at the core of the Dealer Technology Ecosystem, there are now many different systems which all need to share data to ensure customers, vehicles, and parts can be effectively managed throughout the entire online and offline journey. This Dealer Service Provider (DSP) Ecosystem is ever-changing and it is absolutely critical to ensure processes are implemented for secure and efficient data integration.

The DSP choices are changing by the day and it is critical for dealers to understand the importance of secure and effective data integration. There are DSP solutions which focus on the front-end of the dealership and there are solutions which focus on the back-end. Other solutions are aimed at managing customers from online to offline and some are specifically looking to assist dealerships with new/used vehicle inventory merchandising, content management and distribution or to maintain a positive image within the social media and online world.

Whether working with a vendor who offers numerous products or one that specializes in a specific capability, it is important to be sure to understand how data will be integrated and managed across the entire ecosystem.

There is no one-size fits all approach for implementing a DSP solution for a dealership, but it's critically important to align technologies with business priorities and implement data governance processes which support the desired customer experience. Customers are increasingly expecting a seamless online to offline experience which can only be achieved through data integration.

The dealership has a large number of choices when deciding which DSP's will be utilized within their network footprint. DSPs often serve as a "hub" of dealer data, communications, and business operations. When reviewing various DSP offerings, the STAR DIG Dealer Network Infrastructure section can provide guidance on the different functions a system service provider can deliver to dealerships.

3.2 Data Integration & Standards: The STAR Benefit

The STAR organization and the integration standards contained within were created to optimize dealer data integration activities between the OEM and DSP (primarily DMS in the beginning) using the Internet as the main medium.

As with all technology, the Internet has continued to evolve and the infrastructure used to operate businesses using it has undergone a tremendous amount of innovation. These improvements have resulted in an extremely reliable method to integrate business processes and associated systems.

At the heart of all these systems is the data needed to support the desired business process. Vehicle data, parts data, customer data, service data, financial data and many other data groups need to move from one system to the next - and between the dealer (along with the DSP) and the OEM - seamlessly and securely. The STAR data integration standards are open standards which allow vendors and OEMs a method to reduce overall development time and simplify deployments through a set of documents outlining data elements needed to support business objectives (BODs – Business Object Documents).

Over time, these BODs can be enhanced with business definitions/rules and aligned with various data transport methodologies to provide efficient and repeatable data integrations. When STAR began this all important journey, the ecosystem was much simpler. With the dealer technology landscape getting more complicated with every passing year, the standards will truly begin to display the STAR benefit!

3.3 Dealer Technology Landscape (DSP Choices)

It appears that the Dealer Technology Landscape will be in a constant state of change for the foreseeable future. Spending any amount of time trying to define this landscape would only result in a document which becomes outdated shortly after it was published.

In recent years, several new and significant DSP product categories have joined the traditional DMS and made a permanent mark within the automotive retail ecosystem and are worth providing a little of their background information. As with all DSP choices, one should take time comparing capabilities and ensure the solution aligns with the STAR Infrastructure Guidelines.

In additional to comparing capabilities and understanding overall integration, it is extremely important to understand the data management and associated opt-in/out elements with the solution. Complete data governance and usage transparency is crucial for any DSP/OEM solution.

3.3.a DMS

The Dealer Management System (DMS) is a bundled management information system created specifically for automotive industry car dealerships. It has been further adapted (typically as a specialized DMS product) for dealers of heavy equipment, boats, bikes, RVs and power sports equipment. The DMS contains functionality to support the finance, sales, inventory, parts, service and accounting/business office components for the running of the dealership.

Some DMS solutions are offered with onsite central servers, and some are offered leveraging “the cloud” using a software-as-a-service (SAAS) model. Either an onsite or SAAS-based solution could be a fit, depending on dealership needs. One important consideration is the maintenance of the hardware being used to service application needs. SAAS services are generated in the cloud and do not require much maintenance, while onsite solutions often require patch management, upgrades, and general server maintenance.

Although general functionality of both solutions are similar from one DMS to another, specific capabilities can vary. In all cases, it is critical to ensure the solution will support state/local/market/region regulations and OEM brands for the specific dealership group.

3.3.b CRM & Lead Management

The Customer Relationship Management (CRM) and Lead Management systems are used to effectively capture, track and manage online and offline correspondence with prospects and customers.

CRM and Lead Management solutions require integration with DMS Data (Customers) and all Lead Sources (Prospects).

The CRM system provides functionality which assists dealership personnel in managing the customer relationship through the entire customer lifecycle. Customer and Vehicle key dates, Service Appointments and many other aspects can all be managed.

The Lead Management system provides functionality to assign leads to sales and service personnel (or through a defined Business Development Center) for follow-up. These lead follow-up activities are all aimed at driving increased sales and revenue.

Leads (Inquiries) are gathered and stored from many different sources including but not limited to:

- Walk/Drive-ins
- Purchased Online Leads
- OEM Provided Leads
- Phone Leads
- Event Capture Leads

The CRM and Lead Management solutions are also leveraged to generate new business. By aligning dealer solutions with OEM manifests, other DSP solutions (e.g. Equity Mining) and used car needs, it is possible to effectively reach out to existing customers and create additional business.

Dealerships need the infrastructure in place to support leads from tier 3 companies. An effective lead management solution should also take into consideration tier 3 organizations (such as cars.com and truecar.com).

3.3.c Reputation Management

A Reputation Management solution provides functionality to help you monitor, understand, identify, and address what people write online about your dealership.

A Reputation Management solution requires integration with DMS and OEM data sources.

A dealership’s online reputation is defined by the comments found on customer review sites, blogs, websites, and social media sites. The internet makes it easy to find information about a dealership with little effort. In a few clicks, a customer has a snapshot of what a dealership is about, where it’s located, and how customers feel about the dealership overall. In most cases, search results include star ratings and reviews. These ratings and reviews influence a customer’s decision to purchase a vehicle from a dealership.

3.3.d Online Inventory Management

A Dealer Inventory Management solution provides functionality to enable vehicle inventory merchandising, content management and distribution. This includes dealer-directed distribution of in-stock new/used vehicle inventory to web and/or print publications along with vehicle photos, video walk-arounds, pricing, incentives, etc.

A Dealer Inventory Management solution requires integrations with the DMS, third-party pricing tools, lot service providers, Vehicle Description Service Providers (VIN validation and build data) and OEMs.

3.3.e Equity Mining

An Equity Mining solution provides functionality to identify consumers who have equity in their vehicle and then provide them as potential sales leads via a Business Development Center (BDC), internet manager, sales team, or other appropriate dealer representative.

An Equity Mining solution requires integration with DMS Data (Customers), CRM/LM (leads), trade-in sources, bank data (financing & leasing) and incentives.

3.3.f **Service Lane Tools**

Service Lane Tools is a process or workflow-based solution that encompasses functionality that has been traditionally found in separate service-related solutions (i.e. DMS, Online Service Scheduling, service menus, vehicle health checks, etc.). It enables a consistent and seamless customer experience through the stages of 1) scheduling the appointment, 2) service write-up, 3) vehicle in service and 4) service redelivery.

Service Lane Tools requires integration with DMS and OEM data sources.

3.3.g **Dealer Digital**

A Dealer Digital Marketing Package is a suite of retail marketing Services that enable Dealers to deliver consistent, synchronized messaging to consumers utilizing digital and emerging channels. It provides an intelligent network marketing platform with brand and dealer marketing alignment. It also provides analytics supporting multitier marketing spend optimization and Dealer Network performance improvement in marketing and sales processes.

Dealer Digital solutions require integration with DMS, CRM, and OEM data sources.

Core components of a Dealer Digital solution might include:

- Dealer Website (Web and Mobile)
- Search Engine Optimization (SEO)
- Audience Management
- Insights & Analytics
- Asset Management (Images, Videos, etc.)
- Chat
- Appointments

4. Disaster Recovery and Business Continuity

4.1 Overview

Disaster recovery and business continuity is 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 are processes that help organizations prepare for disruptive events—whether those events might include a devastating tornado or simply a 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.

4.2 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	

5. Cloud Computing and Virtualization

5.1 Overview

Important emerging trends in Information Technology can be summarized as a Service-based paradigm and Virtualization. With a "Service-based paradigm", we condense different acronyms such as Service Oriented Architecture (SOA) and the popular concept Cloud Computing (that has relevant business implications). *"The main enabling technology for cloud computing is virtualization. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization."* (Wikipedia)

5.2 Client/Server Virtualization

Virtualization, in computing, means to create a virtual version of a device or resource such as a server, storage device, network, etc. where the "framework" divides the resource into one or more execution environments. Applications and human users are able to interact with the virtual resource as if it were a real, single physical resource. In a dealer environment, the most relevant areas for virtualization are Server Virtualization and Client Virtualization; both of which are interesting and assure consistent savings.

5.3 Cloud Computing

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (NIST definition - National Institute of Standards and Technology)

Cloud computing relies on sharing resources to achieve economies of scale, similar to a utility (like the electricity grid), over a network. At the foundation of cloud computing is the broader concept of shared and standardized services, exploited with a consumption model.

According to NIST, the cloud model is composed of three basic service models.

- Software-as-a-Service (SaaS): the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

- Platform-as-a-Service (PaaS): the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
- Infrastructure-as-a-Service (IaaS): the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Email and CRM are already used by many dealers with a SaaS model. Many DMS providers are already offering something similar to a SaaS model for their DMS. The other 2 models are rarely adopted by dealers- with a few exceptions (e.g. IaaS for disaster/recovery is an interesting option).

6. Training, Process, and Documentation Practices

Many experts will argue that most data breaches are due to human error. In the last two years, studies by Nuspire Networks, IBM, Verizon, and The Ponemon Institute have all concluded the biggest threat to dealer data could be employees. Beyond security, employees are often the cause of network outages, device failure, and slow business operations. Most of the time, the root cause is not poor employees, but rather poor training and documentation. Employees often let in a security incident, do not know how to use systems, and/or cause network failure because they have not been trained on what to do or not to do. This lack of employee training can oftentimes lead back to a lack of documentation.

The following section covers training tips and guidelines from both a technology and a data security perspective. Dealerships are encouraged to adopt training policies and procedures. These policies should be well-documented used with employee training. Documentation, process, and procedure alone can have a positive impact on network operations and dealer data security.

6.1 Employee Training

Recommendation	Specification
Security Training	Have a formal, written, security training program for each employee. Training should cover aspects including social engineering awareness, password management, data sharing policies, and sensitive data handling procedures. Regularly review training programs and adjust for new technologies, dealer business changes, and employee feedback.
Designed Security Responsibility	Designate an employee as program coordinator for your information security program.
Dealer IT Systems Training	Provide formal training for critical applications, hardware, and other dealer IT systems. A well-informed employee can increase productivity, reduce support costs, and improve customer satisfaction.

6.2 Process

Recommendation	Specification
New Employee Access	Have a written, formal, process to grant new employees system access. This should include unique usernames and passwords.
Terminated Employee Access	Have a written, formal, process to remove employees from the dealer IT network, retrieve dealership hardware, and inactivate all employee accounts before they leave.
IT Systems Training	Have a formal program to address training of dealership technologies, applications, and hardware. A well-informed employee can increase productivity, reduce support costs, and improve customer satisfaction.

Risk Assessment	Identify reasonably foreseeable, internal and external risks to the security, confidentiality, and integrity of customer information. Design and implement customer safeguards to control the risks identified through risk assessment.
Third-Party (Vendor) Security Controls	Selection of trusted Service Providers is very important. Select service providers that are experienced in protecting a dealer's customer information.
Security Incident Handling and Response	Have a formal process to respond to security incidents on the network. Cover aspects around identifying security breaches, response, communication and documentation.

6.3 Documentation

Recommendation	Specification
Security Documentation	Create a written security policy that addresses technical, process, and administrative standards for dealing with customer data security. The documentation should include: • Employee training • Incident/ breach response and management • Employee internet usage agreements • Policies & procedures for network monitoring and management
New Employee Documentation	Have a written program for new hires. This should include security training, system training, and a documented process to request IT technical support.
Systems Documentation	Make available training for critical applications, hardware, and other dealer IT systems. A well-informed employee can increase productivity, reduce support costs, and improve customer satisfaction.

7. Glossary

802.11: 802.11 is a group of wireless specifications developed by the IEEE for wireless local area network (WLAN) communications. It details a wireless interface between devices to manage packet traffic to avoid collisions. Some common specifications include the following: 802.11a, 802.11b, 802.11g, 802.11n, etc. The 802.1X standard is designed to enhance the security of wired and wireless local area networks that follow the IEEE standard.

Antenna: A device for transmitting and receiving radiofrequency (RF) signals. Often camouflaged on existing buildings, trees, water towers or other tall structures, the size and shape of antennas are generally determined by the frequency of the signal they manage.

App (Application): Downloadable tools, resources, games, social networks or almost anything that adds a function or feature to a wireless device that are available for free or a fee. Some applications may also offer users the ability to purchase content or enhanced features within the application. Parents may limit their child's ability to download or make these in-app purchases by password protecting those features on a wireless device. CTIA created an application rating system to help inform parents about an application so they can determine if it's appropriate for their kids: http://bit.ly/JtPvve.

Broadband: A transmission facility having a bandwidth (capacity) sufficient to carry multiple voice, video or data channels simultaneously. Broadband is generally equated with the delivery of increased speeds and advanced capabilities, including access to the Internet and related services

Cat5: A twisted pair cable type designed for high signal integrity. Many such cables are unshielded but some are shielded. Category 5 has been superseded by the Category 5e specification. This type of cable is often used in structured cabling for computer networks such as Ethernet, and is also used to carry many other signals such as basic voice services, token ring and ATM (at up to 155 Mbit/s, over short distances).

Cat5e: The category 5e specification improves upon the category 5 specifications by tightening some crosstalk specifications and introducing new crosstalk specifications that were not present in the original category 5 specifications. The bandwidth of category 5 and 5e is the same - 100 MHz.

Cat6: A cable standard for gigabit Ethernet and other network protocols that is backward-compatible with the Category 5/5e and Category 3 cable standards. Cat-6 features more stringent specifications for crosstalk and system noise. The cable standard provides performance of up to 250 MHz and is suitable for10BASE-T / 100BASE-TX and 1000BASE-T (gigabit Ethernet). It is expected to suit the 10GBASE-T (10gigabit Ethernet) standard, although with limitations on length if unshielded, Cat 6 cable is used. Ford Motor Company recommends Cat6 cabling when running new cable or replacing new wired network segments.

DSL (Digital Subscriber Line): A digital line connecting the subscriber's terminal to the serving company's central office, providing multiple communications channels able to carry both voice and data communications simultaneously.

Encryption: Digitally scrambling information so it can be transmitted over an unsecure network. At the other end, the recipient typically uses a digital "key" to unscramble the information so it is restored to its original form.

Hand-held/Tablet PCs: These devices are computers that can be carried by a user. These are typically much smaller than a typical laptop and do not have the full capability of desktop computers, but can still perform most necessary tasks. They will also allow a user to perform work in various locations of a dealership, which can increase productivity.

IEEE (Institute of Electrical and Electronics Engineers): A professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence. It has about 425,000 members in about 160 countries, slightly less than half of whom reside in the United States.(http://www.ieee.org)

LAN (Local Area Network): Local Area Network (LAN) is a small data network covering a limited area such as a building or group of buildings. Most LANs connect workstations or personal computers. This allows many users to share devices such as laser printers, as well as data. The LAN also allows easy communication, by facilitating e-mail or supporting chat sessions.

Malware: Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, and Trojan horses and also spyware, programming that gathers information about a computer user without permission.

Megahertz: Megahertz (MHz) is a unit of frequency equal to one million hertz or cycles per second. Wireless mobile communications within the United States generally occur in the 800 MHz, 900MHz and 1900MHz spectrum frequency bands. (Wi-Fi = 250, 400)

Operating System: The software component of a computer system responsible for the management and coordination of activities and the sharing of the resources of the computer. The operating system (OS) acts as a host for application programs that are run on the machine. As a host, one of the purposes of an operating system is to handle the details of the operation of the hardware. Ford Motor Company recommends Windows 7 Operating system for compatibility with Ford applications.

Patch management: The process of updating servers or PCs. This is often done to update machines to the latest security patches and service packs. Writers of viruses, spyware and other malicious software exploit existing flaws in software loaded on a PC to spread and to do damage. Ford Motor Company recommends dealerships apply critical patches, such as security, as soon as possible.

Rogue wireless access point: A wireless point of entry into the dealership network that is not authorized, secured, or known about by dealer IT, management, and ownership. Any rogue wireless networks must be detected, found, and removed immediately.

Routers: Allow computers from different networks and subnetworks to communicate. In dealerships, routers may be used to connect an OEM LAN, dealership LAN and DMS LAN to the Internet.

Spectrum: The radio frequencies that are designated for a specific use such as personal communications services and public safety.

Spyware: Any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Dealers must deploy systems to detect and remove spyware in order to protect customer data, and network security integrity.

SSID (Service set identification): In computer networking, a SSID is a set consisting of all the devices associated with a IEEE 802.11x wireless local area network. SSIDs must be associated with a specific VLAN. *(See section 4.3 on setting up VLANs for Ford Dealerships.)*

TCP/IP (Transmission Control Protocol/Internet Protocol): A protocol permitting communications over and between networks, the TCP/IP protocol is the basis for the Internet communications.

Trojan (Trojan horse): Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the certain area on your hard disk.

VPN (Virtual Private Networks): A VPN allows a user to conduct secure transactions over a public or unsecure network. By encrypting messages sent between devices, the integrity and confidentially of the transmitted data is kept private.

VLAN (Virtual Local Area Network): In computer networking, a single layer-2 network (switch based) may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN or VLAN. This is usually achieved on switch or router devices.

VoIP (Voice over Internet Protocol): VoIP is not simply capable of delivering voice over IP, but is also designed to accommodate two-way video conferencing and application sharing as well. Based on IP technology, VoIP is used to transfer a wide range of different type traffic.

WAN (Wide Area Network): A general term referring to a large network spanning a country or around the world. The Internet is a WAN. A public mobile communication system such as a cellular or PCS network is a WAN. Dealerships can network remote locations and buildings via WAN technology. In most dealer terms, WAN refers to the dealership Internet service provider.

Worm: A worm is a self-replicating virus that does not alter files, but duplicates itself. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Wi-Fi: Wi-Fi provides wireless connectivity over unlicensed spectrum (using the IEEE 802.11a or 802.11b standards), generally in the 2.4 and 5 GHz radio bands. Wi-Fi offers local area connectivity to Wi-Fi-enabled computers. Ford Motor Company recommends Wi-Fi 802.11n standard.

WPA (Wi-Fi Protected Access): A security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA is not secure and should not be used by Ford dealers.

WPA-2 (Wi-Fi Protected Access II): WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. WPA-2 is the Ford wireless security standard.

Wireless Local Area Network (WLAN): Using radio frequency (RF) technology, WLANs transmit and receive data wirelessly in a certain area. This allows users in a small zone to transmit data and share resources, such as printers, without physically