DIG Quick Reference Guide
2016

Overview

This document – STAR DIG Quick Reference Guide – provides a brief outline of the Star Dealer Infrastructure Guideline (DIG). This document provides a brief guide to industry best practices and recommendations for dealer information technology. The Dealer Infrastructure Guidelines (DIG) and reference document 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. This DIG is intended as a guide to support effective data integration, data protection, system reliability and efficient business processes.

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.

Dealer Network Infrastructure

When to purchase new hardware?

A 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. For recommendations on when to replace hardware, see the STAR DIG section 2.2.a

What to purchase: Consumer Grade Vs. Enterprise grade hardware

Most computer manufactures make 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, often times the total cost of ownership ends up being greater due to the limited functionality, higher failure rates, and more complex support. For these reasons, STAR recommends enterprise grade hardware. For more information on Consumer Vs Enterprise grade hardware, see section 2.2.b of the STAR DIG

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.

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 dealership do not replace desktop or laptop PCs with tablets, but rather augment with tablets when application and function calls 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 version.

Decommissioning & Recycling Hardware

It is the original device owner's responsibility to insure 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 you should follow in picking a recycler:

Recommendation	Specifications
Recycler's Policies & Practices	• Magnetic wiping method for data removal • Storage media should be destroyed by shredding, cutting, incinerating, multiple perforations or crushing. • provide written certification that the data was wiped or storage media destroyed
Certifications	• E-Stewards – www.e-stewards.org • Basel Action Network – www.ban.org • R2 – www.sustainableectronics.org
Company track record	• No environmental or safety violations (citations, fines, notice of violation, consent orders, etc) in the last 5 years
Downstream partners	• Ask if they send used equipment or wastes to other business partners or service providers; these are called 'downstream partners' and should be avoided
Insurance	• A recycler should have general liability and environmental liability insurance.

For more information on decommissioning and recycling hardware, see section 2.2.e of the STAR DIG

Software Recommendations

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. For more information on Operating Systems see section 2.3.a of the STAR DIG

Internet Browsers

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. For more information on Internet Browsers, service packs, and compatibility see section 2.3.b of the STAR DIG.

Software Licensing Recommendations	
Recommendation	**Specifications**
Sharing Licenses	• Do not share a common license. Instead follow software licensing guidelines, generally one per device.
Sharing Logins	• Do not share logins for cloud based software
Software usage	• Avoid having legally licensed copies of the software installed, and not used. • Do not use pirated software
Home Vs. Enterprise	• Do not buy "home" versions of software instead of business class or enterprise class
Software Asset Management (SAM) Program	• Create a Software Asset Management (SAM) program. SAM is the practice of managing and optimizing the purchase, deployment, maintenance, and life cycle of software assets within an organization.

For more information on software licensing, see section 2.3.c of the STAR DIG.

Local Area Network (LAN)

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.)

Wireless Networking

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.

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 has a backup ISP connection from a different provide, using a different technology. See section 2.5c for recommendations on internet back up connections.

Security

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.

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.

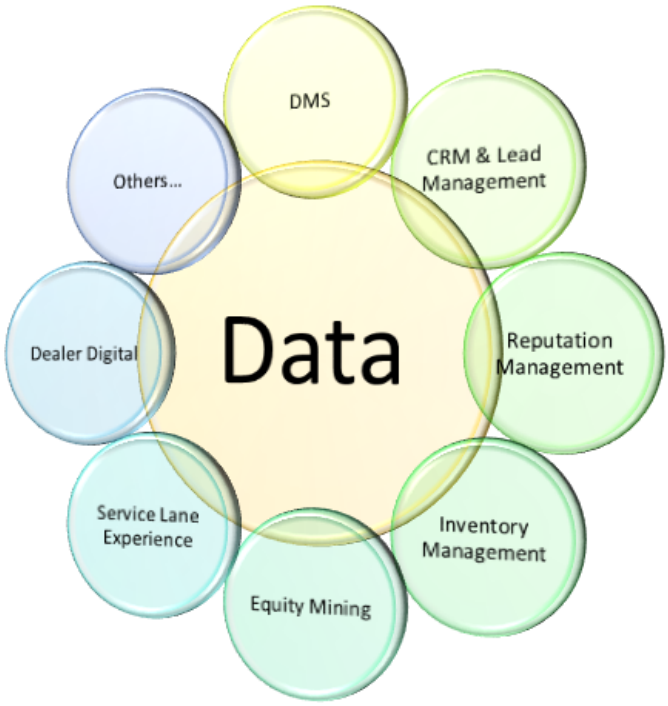
Data Security	
Recommendation	**Specification**
Security Information Event Management (SIEM)	Proactive, real-time security event monitoring that utilizes a SIEM (Security Information and Event Management) service. The SIEM service needs to be able to notify the network administrator in the case of a 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.

Managed Service Providers

Dealers often turn to vendors or partners to help manage, maintain, and secure the dealership infrastructure. 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, scope of services, and any refunds or offsetting charges for missed commitments. See section 2.7 of the STAR DIG for guidelines on managing service providers and SLAs.

Dealer System Providers

The complexity of a Dealership and 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.

There is no one-size fits all approach for implementing DSP solutions 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.

DSP choices (Dealer Technology Landscape)

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 background information. Turn to section 3.3 of the STAR DIG for more information on the following topics:

DMS
CRM & Lead Management
Reputation Management
Equity Mining
Service Lane Tools
Dealer Digital
Inventory Management

Disaster Recovery and Business Continuity

Risk Analysis & Mitigation

To help identify some of the various categories of risk, below is a list of some of the risks that a dealership may be faced with. Review the following: 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 are as follows:

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	

For more information on Risk Analysis and Mitigation, see section 4.1 of the STAR DIG

Training, Process, and Documentation Practices

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.

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.

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.