STAR®

Standards for Technology in Automotive Retail

STAR Dealer Infrastructure Guidelines

2025

INDUSTRY BEST PRACTICES AND RECOMMENDATIONS FOR AUTOMOTIVE RETAIL INFORMATION TECHNOLOGY

Table of Contents

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 teams' 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 supported 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 (e.g., PCs, laptops, handheld devices), routing that data (e.g., routers, switches, firewalls), and providing that data when upon demand (e.g., 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 network 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 partners.
- Current hardware 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.
- Hardware is no longer supported by the manufacturer. Meaning patching, security updates, and software advancements are not performed on the hardware device. When the hardware is no longer supported the dealership is exposed to security and reliability risks.

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

Endpoint Hardware (Desktops, Laptops, and Tablets)

STAR recommendations for dealership desktop, laptop, and tablets have shifted away from broad hardware specifications. This is based primarily because of advancements in hardware processing power, the shift to cloud computing, and the ubiquity of mobility. STAR recommends hardware needs be determined on a use case scenario based on job function. When purchasing new devices, take the following factors into consideration:

1. **Mobility:** Some functions within a dealership require mobility. Other job functions occur primarily at one physical location. Consider needs for mobility when purchasing a new device. Also remember that many mobile devices, such as tablets, run on specific software that may not be compatible with all needed hardware and software. Consider hardware and software requirements before deciding if a tablet, laptop, or desktop is the best choice for that job function.
2. **Software Requirements:** Roles at the dealership will require interaction with different software. Software is often written for specific operating systems and internet browsers. Software applications may also require a minimum hardware specification. When purchasing a new device, understand the software the device will run, and the associated requirements needed to operate that software.

3. **Hardware Accessory Requirements.** Dealerships often need specific accessories to perform a job function. Sales aids, service diagnostics, and other physical adaptors are needed for specific use cases. These accessories are often made with specific software and hardware specifications in mind. If the rob function requires a specific accessory, check with the vendor for requirements before purchasing new equipment.

4. **OEM, DSP, and 3rd party requirements:** OEMs, Dealership Service Providers, and other 3rd party vendors often deploy specific dealership technologies. These technologies (hardware or software) may require specific specifications to operate efficiently. If a dealership device uses specific technologies, check with the technology provider.

5. **Reliability:** Device reliability needs to be considered when making hardware purchases. Some areas of the dealership, such as the service environment, are more prone to device failure. Some job functions are more limited by device downtime. When considering when and what to purchase, take into account the likelihood of device failure, and the impact a failure can have on that job function and dealership business operations.

Beyond use case recommendations, STAR can provide guidance on when to purchase new hardware, and what to purchase when that time comes. STAR provides guidance on "when to purchase new hardware" in the STAR Dealer Infrastructure Guideline in section 2.2.a. When determining what to purchase, STAR provides guidance on Consumer Grade vs Enterprise Grade hardware purchases in section 2.2.b. and a guide for Tablets and Mobile Devices in section 2.2.d.

For more information on dealership hardware recommendations, including tablets, mobility, and hardware decommissioning & recycling please see section 2.2.e.

Network Hardware (routers and switches)

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 802.11ac/ax compatible.

2.2.d Tablets & Mobile Devices

Tablets are handheld devices designed for mobility and accessibility. Tablets do not often 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 or DSP 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, Microsoft has ended support for XP, Vista, and Windows7 operating systems. This includes critical security updates. STAR recommends dealerships do not use Windows XP, Vista, nor Windows 7.

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	22H2	13-Oct-20	14-Oct-25
Windows 11	24H2		
MAC OS X	15.1.1	Versions 14 and below no longer supported.	Versions 14 and below no longer supported.
IOS (for iPad and iPhone)	18.2		
Android	15		

Latest updates/service pack as of January 2025

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
Apple Safari	17	Not recommended for use on Microsoft Operating systems
Google Chrome	131	
Internet Explorer	11	Internet Explorer was retired in June 2022. Microsoft Edge is the browser recommended by Microsoft.
Microsoft Edge	1131	
Mozilla Firefox	133	

Latest updates/service pack as of January 2024

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.

Recommendation	Specification
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. - Additional hardware redundancy can be achieved through a secondary, high availability firewall. - 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.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 (switches) should be housed in a wiring closet or communications room. All equipment should be mounted or secured to a rack or shelf. Some models of switches can house an additional power supply for further fault tolerance.
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. - Implementing SDWAN is a preferred solution that provides failover, optimized traffic features, and keeps configurations stored in the cloud while connecting the dealership to the internet, data centers, and other dealer locations.

2.4.b Dealer Infrastructure and Business Continuity

Dealer infrastructure plays a critical role in disaster recovery and the ability to return to normal network operations. Critical areas of a dealership's network should be in high availability, have redundant infrastructure, or critical backup solutions in place. Star recommends the following infrastructure considerations:

Dealer Infrastructure	Recommendation	Reference
Data Transport/ Bandwidth	Multiple technologies and carriers provide reliable internet connectivity	Section 2.5.c
Wide Area Network	Technologies such as SDWAN provides failover, optimized traffic features, and keeps configurations stored in the cloud while connecting the dealership to the internet, data centers, and other dealer locations.	Section 2.4.a
Local Area Network	High Availability Hardware, redundant power Supplies, and configuration backups ensure equipment failure does not impact business operations.	Section 2.4.a
Data Backup	Data on servers, endpoints, and network equipment should be backed up to another location.	Sections 2.2.c and 2.4.a

2.4.c 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. Note: Check with OEM recommendations for compatibility guidance for OEM specific technologies.
Network standard	802.11ax 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 Service	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. VDSL is another asymmetric technology that can offer speeds up to 52Mbps.	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.
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.

Technology	Description	Speed	Physical Medium	Comments
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.

2.5.b Planning for Bandwidth

Start by understanding the current dealership internet service

Many dealerships are unaware of their current internet technology, speed, and usage. 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.

Stay vigilant

Since bandwidth usage is not static, planning should be an ongoing activity. By gaining visibility into the dealership's usage patterns, an IT administrator can better stay ahead of potential bandwidth limitation before it impacts dealership business performance. It is recommended dealerships set up alerts for utilization spikes, average consumption usage or times bandwidth is unavailable. This will mitigate risks, limit downtime, and allow the dealership to upgrade before a significant business impact.

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 5G 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, 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 Security Policies

The Security Policies framework of the dealership needs to be complete, consistent, and approved by the dealer's management body. It is important to ensure all stakeholders commit to the policies and agree to implement them in all relevant aspects of the dealership.

Policies should reflect the strategy for securing information - not the other way around - and understanding security requirements is the key factor here. The basic focus should be on confidentiality, integrity, and availability of sensitive data and resources including the physical environment, network infrastructure, applications, and data (both physical and digital). However, this is not a complete list, as there are many other considerations. For example, quite often non-repudiation, traceability, or authenticity should be considered.

Moreover, every industry has its own sensitive areas. For instance, we care much more about the integrity - rather than the confidentiality - of an airplane in the air or of a car on the highway in comparison to caring about the confidentiality of the medical history of a patient (which also may depend on the context). Security policies should reflect these considerations.

There are many out-of-the-box policies or framework directives for security from which to select and apply in a company. However, even though this kind of framework can provide a general baseline, a company will need to adjust and develop the policies for application within their business context.

2.6.b Identity and Access Management

Identity and Access Management (IAM) is a critical framework for ensuring that the right individuals have appropriate access to information and technology resources. Identity management involves creating, maintaining, and managing user identities and their associated access permissions. Authentication is the process of verifying that a user is who they claim to be, typically through passwords, biometrics, or multi-factor authentication (MFA). Authorization, on the other hand, determines what an authenticated user is allowed to do, ensuring they have access only to the resources necessary for their role. Best practices in IAM include adopting a Zero Trust approach, enforcing the principle of least privilege, and regularly auditing access controls. These practices are essential for protecting sensitive data, preventing unauthorized access, and ensuring compliance with regulatory standards.

- Zero Trust.
    - Explicit Verification: Every access request is thoroughly verified. This includes verifying the identity of the user, the health of the device, and the context of the request (e.g., location, time of day) before granting access1.
    - Least Privilege Access: Users are granted the minimum level of access necessary to perform their tasks. This reduces the risk of unauthorized access to sensitive information.
    - Assume Breach: The framework operates under the assumption that a breach has already occurred or could occur at any time. This mindset drives continuous monitoring and validation of all access requests.
    - Strong Authentication: Multi-factor authentication (MFA) is often used to ensure that users are who they claim to be. This adds an extra layer of security beyond just a username and password.
    - Continuous Monitoring: User activities are continuously monitored for any signs of suspicious behavior. This helps in detecting and responding to potential threats in real-time.
- Identity management.
    - Establish unique logins: Each member of the organization is provided a unique login for the system and assigned access to the applications and functions necessary for their assigned duties.
    - Maintain accurate user rosters: Network administrators maintain end user rosters and actively delete users upon termination.
    - Strong Authentication Methods: Authenticate users by requiring unique passwords for each application and system the user accesses. Passwords should not be replicated or repeated for different applications, functions or system access. Implement multi-factor authorization (MFA), biometrics or tokenization or any combination to validate the identity of the user upon access request.
    - Actively manage third-party users: Hold third-party users to the same criteria as internal users and have a dynamic process for removal of third-party users as their need to access systems and applications changes.
    - Codify identity management policies and procedures in written form.
- Access management.
    - Define a Clear Access Management Policy: Establish and document policies that outline how access is granted, reviewed, and revoked. This should include guidelines for user roles, permissions, and responsibilities1.
    - Role-Based Access Control (RBAC): Assign access rights based on user roles within the organization. This ensures that users only have access to the information necessary for their job functions.
    - Strong Authentication Methods: Implement multi-factor authentication (MFA) to add an extra layer of security. This helps verify user identities more robustly than just using passwords.
    - Regular Access Reviews: Conduct periodic reviews of user access rights to ensure they are still appropriate. This helps identify and remove unnecessary or outdated permissions.

- Secure Offboarding Processes: Ensure that access rights are promptly revoked when an employee leaves the organization or changes roles. This prevents unauthorized access by former employees.
- Continuous Monitoring and Auditing: Monitor user activities and access patterns continuously. Use auditing tools to track and log access events, which can help in detecting and responding to suspicious activities.
- Identity Federation and Single Sign-On (SSO): Implement identity federation and SSO to streamline access management across multiple systems and applications. This reduces the complexity of managing multiple credentials.
- Environmental Hardening: Strengthen the security of the environment where access management systems operate. This includes securing servers, networks, and endpoints. It also involves prohibiting access to spaces where data and systems are kept from people without a valid need for access to the physical space. Do not maintain data in spaces without controlled access.

The integration of robust identity and access management (IAM) practices is essential for advancing through the three levels of information security maturity. At the **Initial (Ad Hoc)** level, organizations often struggle with inconsistent and reactive IAM processes, leaving them vulnerable to security threats. As they progress to the **Managed (Defined)** level, IAM becomes more structured and proactive, with clearly defined policies and procedures that enhance the organization's ability to manage and mitigate risks. Finally, at the **Optimized (Advanced)** level, IAM is seamlessly integrated into the organization's operations, fostering a mature security culture that continuously evolves to address emerging threats. By aligning IAM practices with these maturity levels, organizations can significantly strengthen their overall security posture and resilience.

2.6.c Patch Management

The operating systems on the local servers/computers require updates from time to time, many of which are due to security risks. Patches sent out by the manufacturer often provide protection from new or previously unknown exploits. It is critical these patches be managed, implemented, and verified to ensure a reliable, secure application. Furthermore, dealerships should pay special attention to the following:

- End of Life (EOL) systems
  - Keeping current with operating systems End of Life (EOL) will assist in making sure the location is not using operating systems that no longer receive security updates or other kinds of updates because the supplier discontinued support.
  - Generally, suppliers provide notice of EOL, and this can always be verified on their respective websites.
- Mobile devices
  - Mobile devices will often leave the protection of a dealership network and connect to another, often less secure network. Because of this, these devices can be considered more vulnerable. It is important that mobile devices are patched quickly to limit risk and exposure to threats and vulnerabilities.

2.6.d Security Awareness Training

The vast majority of security incidents, including data breaches, are the result of human error – like clicking on a phishing email, for example. Just as technicians are trained in the latest vehicle developments and salespeople on new vehicle features and sales techniques, all your employees must be trained on how to protect your business from theft, data breaches, and other security issues.

The goal of the training program is not just to educate your employees, but to influence their behavior. You want them to become a human firewall for the company.

Security should not be boring – if people do not pay attention, the message will not permeate – so do not be afraid to get creative with the training and awareness program. Humor, real life examples, and contests and games are a few ways to keep it interesting and gain employee engagement.

To keep employees engaged, consider using shorter, online security training modules more frequently rather than one, long training sessions. This approach helps keep training up to date on the latest developments in malware and attacks.

- Training should be annual, at a minimum, and cover topics that include:
  - Social engineering awareness: phishing, Business Email Compromise (BEC), vishing, ransomware, safe web browsing
  - Passwords
  - Sensitive Data – PII, PCI, PHI, etc. – and data handling
  - Data sharing and acceptable use policies
  - Data protection and destruction
  - Mobile device security
  - Safe social networking
  - Workplace violence
  - Security-related company policies
- Further training may be necessary depending on the employee's role in the company. For example, employees that handle company finances may benefit from understanding the unique ways they are targeted by cyber

criminals for the access they have to bank accounts. Consider role-based training to help employees understand the role they play in protecting the company in their daily activities.

  - Use security awareness materials in break rooms and other employee-only spaces such as posters or fliers reminding employees of safe handling of customer data, social engineering awareness, training reminders, etc.
  - Use company newsletters, emails, live training sessions, and other company functions to continually reinforce the security message.

- Regularly review training programs and adjust for new technologies, dealer business changes, and employee feedback.

- Resources. These can be free or paid, but some of your business partners may offer online security training for your employees.

  - DMS provider
  - Insurance provider
  - Accounting firm
  - Legal firm

- Other resources:
  - How to Make Cybersecurity Training Accessible
    - https://www.staysafeonline.org/articles/how-to-make-cybersecurity-training-accessible?utm_source=chatgpt.com
  - SANS Ouch – a free monthly security newsletter for employees
    - https://securingthehuman.sans.org/resources/newsletters/ouch/2016

2.6.e Compliance with Federal Legislations

Ensure the dealer complies with all federal, state, local, and industry regulations for financial and retail institutions such as the Gramm-Leach-Bliley Act, Safeguards Rule, PCI DDS, etc.

- Gramm-Leach-Bliley(GLB) Act and Safeguards Rule
  - The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. The Gramm-Leach-Bliley (GLB) Act requires businesses defined as "financial institutions" to ensure the security and confidentiality of sensitive information. Because dealers lease and lend (even if through a 3rd party), they must adhere to the GLBA Act.

  - The Safeguards Rule was issued by the Federal Trade Commission (FTC), as part of the GLB Act. The Safeguards Rule requires financial institutions to have measures in place to keep customer information secure.

  - For more information on these legislations and the requirements, please visit: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

- Payment Card Industry Data Security Standard (PCI DSS)
  - PCI DSS is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise.

  - All merchants storing, accepting, processing, and/or transmitting cardholder data must comply with technical and operational requirements set forth by PCI DSS. All dealerships must adhere to the PCI DSS. However, there are different requirements for reporting and auditing for dealerships based upon merchant level. Merchant level is determined by the number of credit card transactions at the dealership. For more information on PCI DSS and these requirements, please visit: https://www.pcisecuritystandards.org

- Additional Resources
  - The following organizations have information to help implement appropriate safeguards for data:
    - Computer Security Resource Center National Institute for Standards and Technology (NIST) - http://csrc.nist.gov
    - National Strategy to Secure Cyberspace, Department of Homeland Security - http://www.dhs.gov/files/publications/editorial_0329.shtm
    - The SysAdmin, Audit, Network, Security (SANS) Institute the Twenty Most Critical Internet Security Vulnerabilities - www.sans.org/top20
    - CISA Resources and Tools
      - https://www.cisa.gov/resources-tools
    - Carnegie Mellon Software Engineering Institute CERT Coordination Center - www.cert.org
    - Star Risk Assessment Questionnaire - https://www.starstandard.org/index.php/risk-assessment-questionnaire-2/

2.6.f Network Security

Dealerships need to focus on the security and data integrity of the dealership's local area network (LAN). This starts with policies on network usage for employees and guests. These policies should include what data each user has access to, what resources on the network each user can access, and where data is stored on the network. The policies should also deliberately state which devices company data is stored on. See section 2.6.a for more guidance on security policies and practices.

Beyond policies, the network should be configured and segmented as securely as possible to avoid unwanted access. Use the following recommendations when configuring and securing the dealership network.

Recommendation	Specification
Firewall/ UTM	A fully-managed security device that continually monitors threats through Intrusion Detection system "IDS", 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) Because of the importance of the Firewall, and the fact it is often in the data path for most dealership traffic, STAR recommends a backup device in the case of failure. To limit downtime, dealers should consider a solution for automatic failover to the back-up device in the case of a hardware failure.
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.
Security Information Event Management (SIEM)	A SIEM solution provides visibility beyond AV or firewall protection. The ultimate goal of a SIEM solution is to collect and inspect network security traffic to find indications of compromise. This indication should be sent, as an alert, to a qualified resource to perform investigation and potential remediation activities immediately. It is important to note that the adoption of SIEM software alone is not adequate to protect the dealer network. Dealerships must have processes and resources in place to respond to the information generated by the SIEM technology. General guidance for dealership security information management is as follows. Dealerships must have: • Proactive, real-time event monitoring that utilizes a SIEM service.

Recommendation	Specification
	• SIEM needs to be able to collect data with capability to aggregate and correlate varying security data from the network in real-time. • The SIEM service provider 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).
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.
Wireless Detection System	Scan, identify, and remove any rogue wireless access points that may be on the retailer network. A rogue wireless access point is defined as a wireless point of entry into the dealership network that is not authorized, secured, or known about by 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.
Continuous Monitoring	Continuous monitoring provides real-time visibility and evidence that security controls and data protection measures are working to detect and prevent threats. Use continuous monitoring technologies, processes, and procedures to ensure the dealership has the capability to alert and respond to attacks and vulnerabilities.
Multi-Factor Authentication	Implement Multi-Factor Authentication (MFA) for all privileged accounts and users needed remote access. Use MFA for any individual (employee, vendor or customer) who needs to access systems that contain customer information.

2.6.g 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 the most current virus signature updates • Actively monitor for viruses • Quarantine and eradicate infected files

Recommendation	Specification
	• 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
Endpoint Detection and Response Platform	• A singular endpoint protection platform (EPP) and endpoint detection and response (EDR) solution should be deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. Alerts from this service should be responded to immediately to mitigate risk and potential data loss. The service offering should provide cross-platform visibility into endpoint/server activities as well as: Threat Detection through static and behavioral AI engines and HIDS within the endpoint agent • Threat Containment and Remediation Guidance • Activity Reporting and Threat Hunting • Cross Platform visibility into process execution, network communications, file access, applications, DNS requests and encrypted web traffic

2.6.h Email Security

Overview: Email security is a critical risk for many of the world's largest organizations. Today, 91% of all successful attacks on enterprise networks involve the use of email. An email security solution will provide inbound and outbound content inspection, encryption, and security alerting to mitigate many of these risks.

Outbound Email Security: Identify and respond to malware, inappropriate emails, unauthorized content, and company-private information before it leaves the network.

Inbound Email Security: Apply filters to stop malware, phishing, or malicious emails before entering the network.

Encryption: TLS Email Encryption is recommended to make it more difficult for third parties to read email in transit.

2.6.i Application Security

Below, assume that all applications are acquired from external vendors and deployed either without any modification, or only a small customization is applied. Moreover, by an application, it is understood to be business applications, and the application security is to make sure that all data processed - and all business functions offered by the application - are protected appropriately.

- Areas and key activities
  - Perform an inventory of applications. Document what applications are on the dealership network, what their purpose is, who is responsible, and how to get support. Perform Business Impact Analysis (BIA) including information classification to understand business criticality and apply correct prioritization. This catalog will also help in finding and eliminating rogue applications that can become a threat to the dealer network and data security.
  - Protect processed information in transit and in storage. Make sure that sensitive and critical data is well protected both from a confidentiality and integrity perspective. Review both application-to-application integrations as well as internal communication applications, especially connections to database, which are very often forgotten. If needed, make sure correct cryptography is used for protection in storage. Finally, make sure information flows are protected from an end-to-end perspective.
  - Consider additional business requirements such as authenticity, non-repudiation, or traceability; often required to meet privacy regulations (e.g., GDPR).
  - Apply the Defense in Depth principle by introducing accurate security zones setup and application components placement, additional infrastructure services like reverse proxies or web application firewalls, and access control layers like multi-factor authentication, etc.
  - Introduce the appropriate identity and access management strategy (see more in the IAM section). Apply the least privilege and need-to-know principles.
  - Expect from a supplier the result of an application vulnerability scanning conducted by an independent third-party company. Make sure all identified high and medium risks are addressed.
  - Part of a security strategy is also to make sure that business transactions are handled without errors and on the expected level of quality. By that, one can expect a supplier company to provide test results or audits reports.
  - Introduce processes for handling incidents, access requests, etc. Consider introducing monitoring of business applications to trace or even prevent unwanted events. Usually this is a part of an IT service management implementation.
  - Perform, on a regular basis, threat modeling activities to make sure application landscape risks are documented, mitigated, and kept under control.
  - Apply application updates and patches as soon as possible to limit exposure to potential exploits.

2.6.j Mobility

This area is strongly connected to other areas like application security or email security. However, it is considered separately due to the additional risks it introduces by much less control of the types of devices defined. Mobile devices are defined here as smartphones, tablets, laptops, and any other specialized devices which processes or stores company data.

- Areas and Key Activities
  - Create policies and procedures for who, when, and how to remotely access the company environment and which parts (network, servers, applications, etc.) For instance, a policy can allow smartphones and tablets to access an external company network and restrict access to the internal company network; and allow access to the internal company network for managed laptops over VPN. Deploy an appropriate technical solution to support established approach.
  - Define what information can be processed and stored on the mobile devices; be sure to include considerations related to managed and unmanaged devices.
  - Introduce policies, procedures, and technical capabilities to define what software can be installed and executed on all types of mobile devices. In the case of unmanaged devices, introduce conditions where company data is not exposed to unacceptable risks (e.g., by installing solution like MobileIron or Microsoft iTunes for smartphones).
  - Access to devices should be restricted, requiring user authentication. Most devices can be locked with a screen lock, password, or PIN.
  - Apply the appropriate identity and access management strategy.
  - Make sure about the correct configuration and hardening of device and operating system (e.g., BIOS password, device level encryption, availability of USB and SD ports). Make sure that (especially in case of Android and iOS devices) the device is not rooted and jailbroken.
  - Keep an updated and, preferably, centrally managed antimalware software both on laptops and smartphones.
  - Update the mobile OS with security patches. More information on patch management can be found in section 2.6.c.
  - Apply appropriate encryption of data both on laptops and mobile devices with special care of key management for decryption.
  - Review all connectivity methods, being careful with automated wireless connectivity since passwords may be exposed as well as man-in-the-middle attacks can be executed.
  - Enable remote data wipe option if available.
  - Regularly back up the mobile device.
- Bring Your Own Device (BYOD) policy considerations
  - When the mobile devices used by employees/contractors for business purpose are not provided by the dealership but are the personal property of the employee/contractor, a detailed BYOD policy is necessary and should address the following key aspects in addition to the areas and key activities already mentioned:
    - Designate what mobile phones, tablets, etc. are permitted, old devices may not have the level of security needed to adequately protect business private data.

- Ensure it is clear that ALL data gathered in the course of business is the property of the business.
- Identify which apps are not permitted on the device.
- Use encrypted password lockers in lieu of browser based unencrypted password managers, especially for business application access.
- Require Multi-Factor Authentication (MFA) for access to business networks.
- Implement software/applications that separate personal use from business use such as a browser application that is controlled by the company Information Technology team.
- Define limitations on business data use and deletion when no longer needed for business use.
- Make clear the device wiping policy in the event of an information security incident, wiping may result in personal data loss such as pictures and personal contact information.
- Define requirements for lost device reporting and capability for remote wiping in the event a device is lost or stolen.
- Make clear that BYOD are subject to monitoring and users should have no expectation of privacy in regard to business usage or business data.
- All business data is the property of the business and will be accessible at the request of the business.
- In the event of employment termination, personal device data cleansing must be part of the off-boarding process. Businesses should have remote access capability to wipe company private data from a device in the event an employee departs without notice.
- Require device encryption and the use of VPN for business use.
- Implement training on the proper use of Personal Devices for business and the policies to define the proper use of business applications and business data with personal devices.

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 Service Level Agreements (SLA)

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

2.8 Data Management

2.8.a Data Backup

Having a backup of dealership data is critical for business continuity. It is common for data availability to become a serious problem due to cyber security incidents, physical incidents, or human error. When these incidents occur, it is important dealerships have a backup read, and plan to restore. STAR recommends dealerships perform a full and incremental backup at regular intervals to ensure data availability and redundancy.

Data Backup	Data on servers, endpoints, and network equipment should be backed up to another location.	Further reference: Sections 2.2.c and 2.4.a

2.8.b Data Security (Encryption)

Encryption in IT networks is the process of converting data into a secure format that can only be accessed or decoded by authorized parties. Data encryption guarantees that information remains accessible only when necessary and to the designated recipients. STAR advises dealerships to implement encryption across wireless networks, email communications, endpoints, and remote (VPN) connections.

Use the following guidelines when using encryption across your dealership architecture.

Wireless Encryption	WPA2 with RADIUS authentication and AES Encryption. Note: Check with OEM recommendations for compatibility guidance for OEM specific technologies.
Email Encryption	TLS Email Encryption is recommended to make it more difficult for third parties to read email in transit.
Endpoint Encryption	Apply appropriate encryption of data both on laptops and mobile devices with special care of key management for decryption.
VPN Encryption	Require device encryption and the use of VPN for business use.

2.8.c Artificial Intelligence (AI) Governance

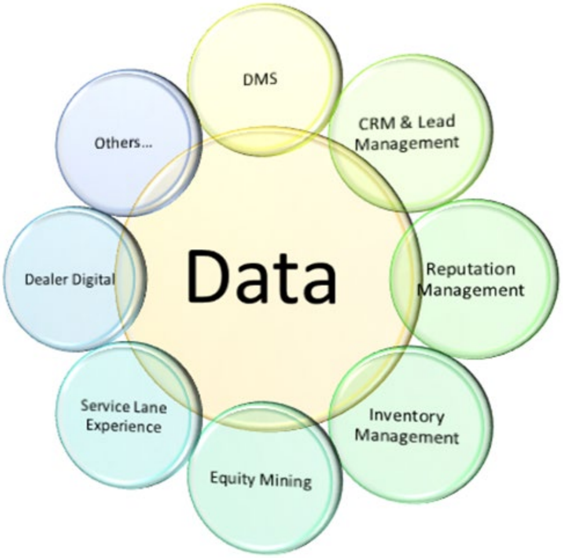
AI Is a great tool to improve dealership efficiency, gain additional intelligence, and perform advanced data analysis. However, the use of AI in the dealership space carries concerns for dealer, customer, and OEM data security. When using AI tools, take into account the following considerations:

- Data anonymization and minimization: Anonymize personal data, collect only necessary information, and implement data retention policies to reduce risk.
- Secure AI model management: Keep models separate from production systems, implement version control, and regularly test for vulnerabilities.
- Vendor security assessment: Thoroughly vet AI vendors, ensure regulatory compliance, and regularly audit their security measures. + Ensure that all vendors’ data governance and security requirements are consistent with your own policies and regulatory requirements.
- Employee training and awareness: Provide regular security training, educate staff on threats, and foster a culture of security awareness.
- Data sharing, ownership, and use considerations. Ensure data given or shared with an AI model is not being shared, sold, or used for other purposes than the intended dealership use case.

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 DSPs 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, so it is 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 is 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 leads 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 is 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 representatives.

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 procedural steps 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 ahead of 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
- Internet disruption or failure
- 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 onsite or offsite. 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 of 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 to use the provider's applications running on a cloud infrastructure.
- Platform-as-a-Service (PaaS): the capability provided to the consumer 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 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 previous 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 a 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 and 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. Appendices

7.1 Dealer Security Policy Guide

The Security Policies framework of the dealership needs to be complete, consistent, and approved by the dealer’s management body. It is important to ensure all stakeholders commit to the policies and agree to implement them in all relevant aspects of the dealership.

Policies should reflect the strategy for securing information - not the other way around - and understanding security requirements is the key factor here. The basic focus should be on confidentiality, integrity, and availability of sensitive data and resources including the physical environment, network infrastructure, applications, and data (both physical and digital). However, this is not a complete list, as there are many other considerations. For example, quite often non-repudiation, traceability, or authenticity should be considered.

Moreover, every industry has its own sensitive areas. For instance, we care much more about the integrity - rather than the confidentiality - of an airplane in the air or of a car on the highway in comparison to caring about the confidentiality of the medical history of a patient (which also may depend on the context). Security policies should reflect these considerations.

There are many out-of-the-box policies or framework directives for security from which to select and apply in a company. However, even though this kind of framework can provide a general baseline, a company will need to adjust and develop the policies for application within their business context.

General Guidelines

- Make sure there is a shared understanding with Management as to what needs to be protected as well as the ambition level regarding data protection. On the one hand, it is important that policies guarantee an expected level of protection. However, it is also particularly important that the policies are not so restrictive as to constrain the company from doing needed business.
- Make sure policies are aligned with laws and regulations (e.g., in the privacy area or industry-specific regulations).
- Develop policies to reflect actual and achievable security practices. It is better to have a small set of rules rather than a comprehensive document that is impossible to follow. Just in case the actual state is far from ambition level, develop a transition plan agreed upon by all key stakeholders to take an organization from as-is to the expected to-be level. It is especially important to develop an effective communication plan as a part of the overall security program.
- Policies should not be changed too often (to include the manner and language in which they are expressed). However, if needed, appropriate changes should be applied as they should always reflect current security requirements and information security strategies.
- Policies should be expressed in such a way that there is no room for exceptions. This is related to both the commitment from all stakeholders to follow the policies as well as to the language. Otherwise, especially when many exceptions are allowed, the question may become whether the Management is really committed to the policy and/or the policy truly reflects the company's strategy for information protection.
- Policies should be expressed in such a way that there is no room for interpretation. In addition, policies need to be supported by guidelines, processes, procedures, roles with responsibilities, and interpretations so it is clear what to do in specific cases. It should also be clear to whom to turn to in case an interpretation or a decision is needed. It is also a good practice to maintain knowledge base articles.
- Make sure appropriate solutions and technologies are available to support policy expectations. For instance, when a policy requires two-factor authentication in specific circumstances, then it is important the existing IT environment allows for an implement to this additional level of protection.
- Introduce a dashboard to track the level of policy implementation, allowing for reliable risk management as well as prioritization of efforts.

Guidelines with examples of policies deemed especially valid from a dealership perspective are as follows.

7.1.1 Acceptable Use Policy

Outlines the acceptable use of a business's physical and digital resources. Covers also ownership and control. Emphasize examples of prohibited activities.

7.1.2 Asset Management Policy

Assets represent everything what has value to the organization. Company assets are considered as both physical and logical dimensions.

Physical. Servers, hard disks, routers, mobile phones, removable media like DVDs or USB sticks, for example. It is important to keep track of the asset lifecycle with special focus being given to asset disposal and re-use.

Logical. It is important a company develop standards governing appropriate data collection, retention, and use. These standards should consider what information is collected, how long it is kept, how it is stored, who may access it, and how access is achieved. This is very connected to the increased role of privacy regulation in different countries.

Additionally, an information classification policy with clear information ownership and protection requirements at different levels should be developed. It is so very important, it is sometimes considered in a separately, identifiable policy.

7.1.3 Business Applications Policy

Introduce a business application classification policy. Describe the requirements for protection on the application level for different levels of criticality (e.g., security zones placement, connectivity methods, identity and access control, applying defense in depth, fail securely, least privilege, and similar principles). Include the expectations regarding application architecture, communication with other systems, and separation of data between customers. Define expectations toward cloud-based solutions (which are becoming more and more popular).

Other aspects to specify is the way in which an application is procured by the company, what are the mandatory steps, what are the common requirements towards suppliers both functional and non-functional (e.g., SLA, security, identity management, integrations). Define expected audits of the acquired application (e.g., Pentest or Vulnerability Scan reports). Support policies with templates and guidelines to be shared with suppliers.

7.1.4 Electronic Communication Policy

In today's technological age, companies have many options for communication and exchange of information. However, risks are associated with these options. For instance, one may use a cloud service to communicate but it is also collecting data with malicious intention. It is important to regulate electronics communication such as emails and instant messaging, using boards like Trello, file exchange over Dropbox, and similar solutions and platforms.

7.1.5 Identity and Access Management Policy

One of the most critical areas. More details can be found in the relevant section of this guideline. Password policy should be included in this section.

7.1.6 Security Incidents Management Policy

There is no IT environment that can be secured 100%. A company needs to be ready for when there is a security incident. The Security Incidents Management Policy should be part of - or contribute to - overall incident management. Provide the definition of a security incident, introduce processes and procedures (i.e., response plan) for what to do in case of a security incident (depending on the incident category, e.g., hacking, wrong behavior, equipment failure), and the criticality. Define the exact procedures for response and action. For example:

- If a computer is compromised, disconnect it immediately from the network.
- If someone is entering without an access card, ask about identity.
- Consider further forensic investigation.
- Consider emergency fixes to support Service and Business Continuity Plans.
- Consider who to notify in the event of an incident, both inside and outside the organization. The following parties may need to be informed: consumers, law enforcement, customers, and credit bureaus and other businesses that may be affected by the breach.

- Quite often there are also laws and regulations which require a specific behavior in case a data breach occurs and will depend on the country, state, and industry.

Policy may also expect to introduce appropriate technical solutions to support policy implementation.

More specific information on incident response can be found at: https://www.sans.org/reading-room/whitepapers/incident.

Sample incident handling forms and documentation can be found at: https://www.sans.org/score/incident-forms.

7.1.7 Network Policy

Network policy is another very important aspect of the overall security. In development of a network policy, it is recommended to consider the following aspects:

- Define network zone classes with supporting organization (zone owner, zone operator, etc.), assign level of trust to every class, define allowed connections between different trust levels. Introduce more restricted network segments for more sensitive applications and data.
- A list of the network devices and the associated configurations as well as what is to be allowed to connect and to where.
- External network connections, VPNs (both for employees and external partners)
- DNS including naming structure as well as supporting infrastructure and scope
- Firewalls, reverse proxy, and proxy configurations (e.g., all outbound traffic to go through a proxy, all sensitive inbound traffic to go over the reverse proxy)
- Wireless classes and standards on authentication and protection in transit. Separate, specific, and very limited segments for customers.
- Remote maintenance
- VoIP, telephony, and conferencing

7.1.8 Risk Management and Audit Policy

Define the risk framework and supporting auditing considerations. Describe the requirements for risk assessment and audits of the business' information and resources.

7.1.9 Threat and Vulnerability Management Policy

A Vulnerability assessment/scan will identify security weaknesses in your computer, network systems, and possibly applications. It is performed with tools that will automatically scan your environment of computers, applications, and network components for what are currently known vulnerabilities for the purpose of exposing whatever vulnerability it detects. These scans are also performed with the administrative credentials needed to perform the secure diagnostics within the systems that only an administrative level can access.

The outcome would provide a severity level and promote a recommended remediation action for each detected concern. These scans should be run on a periodic basis, with a minimum of annually, but recommended to be at least twice yearly or more.

A penetration test (“pen test) is a method of simulating a real-world attack, thus evaluating the security of a computer system and network environment. It is not performed with any administrative access as though to emulate an unauthorized hostile actor. It is different than a vulnerability scan in that it will attempt to find an actual vulnerability and exploit it if present. The pen test will attempt to replicate malicious methods of breaching these systems to show how the threat may disrupt, stop, overtake, or steal from those systems, but it would do so in a manner that only proves it could perform those actions without actually harming the targeted systems. Internal systems that can be reached from the Internet should be assessed from an external (Internet based) point of access, from a system emulating a hostile entity attacking from afar, from outside the company network, like an example of having a hacking attempt launched from a foreign country. Penetration tests may use some automated tools but are orchestrated with a knowledgeable professional skilled in using such tools and tactics. Social engineering attacks are also included in this test to determine if the human errors may expose a weakness and provide a successful attack vector, exposing access to systems and data that shouldn’t have been provided/exposed. Additionally, it is always recommended to perform the physical penetration test (attack, assessment) from within the network as though the threat/attack has been launched from within the organization’s environment (as though the attack is successfully bypassing or thwarting the perimeter defenses).

Objectively, both the vulnerability scan and the penetration test should be run on a regular basis. The cycle would be to perform the vulnerability scan to identify and remediate the found vulnerability issues. The intent of that is to ideally thwart the action of the subsequent penetration test which is attempting to defeat the security by exploiting the vulnerabilities that may exist/remain.

Note that a high-quality endpoint protection installed on all end point computers/laptops/servers/tablets is a prescriptive best practice to reduce vulnerability, to provide continuously monitored threat protection, prevention, and notification. Endpoint protection that provides instantaneous communication to a security operation center (SOC) for immediate review by security professionals is the best solution for this protection to be most effective.

For a variety of sample Security Policy templates, please visit: https://www.sans.org/information-security-policy.

7.2 Identity and Access Management Guide

Cover identity and access management in a comprehensive way. Start with introduction and basic concepts followed by subsections: identity management, authentication, authorizations and why they are so important, access management process, end users and physical consideration, and protection levels. Close with an introduction to the three levels of maturity.

7.2.1 Introduction

Gartner, Inc. defines Identity and Access Management (IAM) as a security discipline that enables:

- the right individuals to access
- the right resources at
- the right times for
- the right reasons.

Even though the definition is quite simple, it captures the essence and implies many considerations in different areas.

7.2.2 Basic Concepts and Definitions

To set a baseline, define the basic terms related to Identity and Access Management.

- **Entity**: a real person or information system
- **Identity**: entity in a specific context (e.g., at work or in social media)
- **Identifier**: set of attributes which identifies identity (e.g., SSN, email, fingerprint)
- **Authentication**: a process of confirming identity claimed by an entity (e.g., by providing password)
- **Authorizations**: set of permissions assigned to someone or something (e.g., "you are authorized to see the medical records of patient XYZ")
- **Accounting/Auditing**: history of what happened

The above is to be considered in both physical and logical dimensions where physical refers to limiting access to buildings, rooms, and other physical IT assets, and logical refers to limiting access to the virtual computer world such as connections to computer networks, information systems, files, or data. Once the above is implemented, introduce the key element in this puzzle.

- **Access control**: is to make sure authorization rules are executed. One can think of it as the implementation of authentication, authorization, and accounting (AAA) in both physical and logical dimensions.

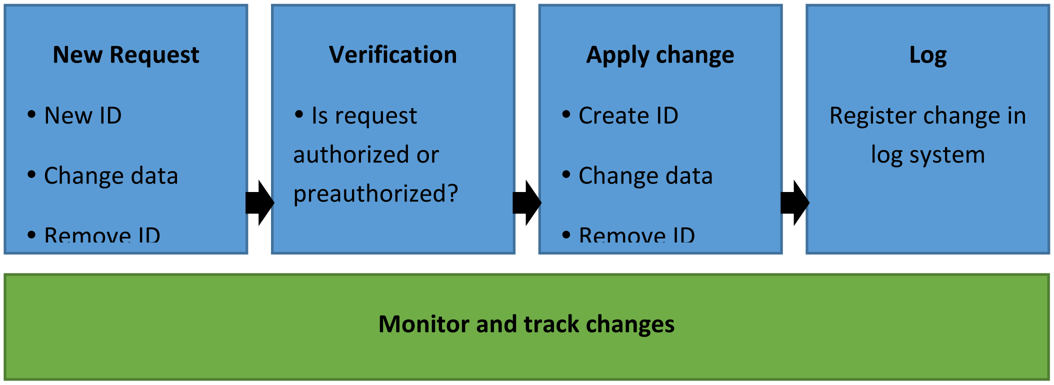
7.2.3 Identity Management

The following aspects of the identity management should be carefully considered:

- Lifecycle of identities
- Management and storage of identities
- Password management
- Identity Federation

Lifecycle of Identities

Lifecycle should be considered from the moment a relationship starts till the moment when it is terminated and monitored over time for context changes (e.g., employee is changing assignment). The process can be illustrated as follows:



Emphasize the following key aspects:

- Limit the number of identities related to a specific entity and centralize management of them (e.g., try to avoid situations where there are application-specific accounts).

- Try to avoid group accounts. In case it is really needed, again, make sure that each one has its own custodian responsible for it.
- Remember that identities are related not only to end-users, but also to services or networks and these kinds of identities need to also be managed and maintained with care. Make sure that every non-personal identity has its own custodian responsible for it.
- Make sure storage of identities is protected, especially when confidential information is stored. Usually, passwords are referred to as an example, but it can also refer to sensitive user information (e.g., GPS coordinates of visited locations).

It is recommended to follow common market standards and security protocols as well as products.

Password Management

Passwords need to be secured both in transit and storage. Additionally, procedures around passwords need to be designed with care. Storage of passwords can be considered from two perspectives.

- **From the server side -** where identity is managed (e.g., Active Directory, business application, etc.).
    - Key aspects
        - Password must not be stored in a plain text and - in case it is encrypted in a reversible way, keyed for decryption needs to be protected in a correct way.
        - All vendor-supplied default passwords must be changed before any information system is put into operation.
- **From the client side -** where a password is used to access resources. If there is a need to store a password, it is highly recommended to store that in an encrypted form (e.g., in a KeyPass application, encrypted Excel file). Then, it is important to protect the master password in a secure manner. It is particularly important to discourage employees from writing down passwords and keeping them in a place visible to others (e.g., on a Post-it Note close to the workplace)
        - divulging passwords to anyone unless absolutely necessary (e.g., helpdesk assistance); and then remembering to change the password after divulging.

  All passwords should be promptly changed if suspected of/are being comprised or disclosed to vendors for maintenance/support.

  It is also important to make sure that all backups where passwords are stored are also secured with care.

  Common procedures which need to be designed in a secure way:

        - Sending the initial password in a secure way
        - Password recovery in case it is forgotten
        - Unlocking in case it is locked
        - Self-service for password change
        - Policies around password lifecycle (see policies section for passwords);
          but remember that too restrictive policies can also have negative consequences.

Identity Federation and Single Sign On

Just in case a company is established with other partners on the IT systems level, it is worth a look at the Identity Federation policy. In short, it is about sharing the same identity between companies based on some level of trust. There is a set of mature technologies supporting the approach. These are the immediate benefits:

- Single Sign On: the end user needs to authenticate once and gets access to a number of applications (without a need for re-authentication)
- Less cost related to managing identity lifecycle
- Less risk related to the need of keeping separate identities by an end user

In the end, a calculation needs to be performed to determine whether it is worth the investment in Identity Federation in a specific context.

7.2.4 Authentication

The most common proof in authentication is the password, but there is also a problem: passwords are hard to remember. Therefore, it has become increasingly popular to use passphrases instead. One needs to remember that recommending passphrases requires changes in policies as well as IT systems to support the new policies.

There are other options to authentication than the password such as biometry, one-time passwords, or smartcards supported by RSA Tokens, mobile applications like Google Authenticator, or Yubikey. Every method is usually classified into one of three categories:

- Something you know (passwords, visual patterns)
- Something you have (smartcard, RSA token, smartphone)
- Something you are (biometry, behaviour)

There are two (2) reasons for applying different authentication methods:

- Better user experience (e.g., biometry)
- Better security (smartcard)

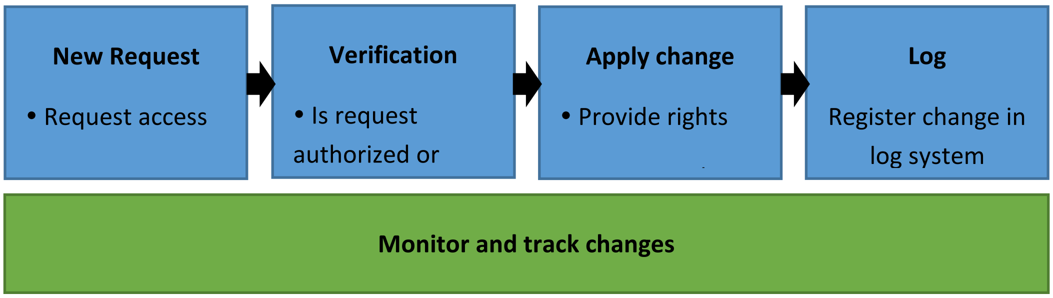
When two or more methods from different categories are combined, this is defined as ***multi-factor authentication*** which is about increasing the level of security.

7.2.5 Authorizations and Access Management Process

Correct authorizations - i.e., permissions' definition and its representation in IT systems - are one of the most important of the overall IT security landscape. The following aspects should be correctly secured:

- Define a structure of roles and access levels.
- Define a set of permissions for given role.
- Make sure authorizations are documented and easily accessible.
- Make sure authorizations are implemented in access control systems.
- Access requests are approved by correct people, and it is clearly defined who are approvers
- Monitoring and reviews (audits) of access rights and authorizations

In addition, the ***Access Management Process*** needs to be established and implemented to make sure that defined authorizations are applied in every place at any point of time. The process is similar to the identity Lifecycle Management process and can be illustrated as follows:


New Request
• Request access
Verification
• Is request authorized or
Apply change
• Provide rights
Log
Register change in log system
Monitor and track changes

The key elements of such a process which should be considered:

- Access is revoked or modified anytime an employee departs the company or changes positions.
- Access should be updated in a timely manner reflecting business needs.
- Access should be reviewed periodically on a documented cadence (quarterly, semi-annually, annually). This evaluation, not prompted by employee exit or transition, is to determine if the level of access presently granted corresponds with the person's position in the business. Please note that frequency of reviews may vary depending on asset criticality which are protected.
- A good practice is also to apply "need to know" principle i.e., access to resources should be given only if there is a business need.

Once again, the importance of monitoring and auditing authorizations and access rights, especially to make sure that access removal is implemented correctly, cannot be overemphasized. Unfortunately, it is quite common that access rights are provided and then never removed.

7.2.6 End Users and Physical Consideration

It is a common knowledge that most problems with security are often caused by incorrect user behaviour. (The ones related to the logical dimensions (like clicking dangerous emails) are covered in other sections.) The elements related to physical access control follow and should also be the basis for appropriate education strategy.

- Server/equipment rooms should be locked. Employee access should be limited to only those who have a legitimate business need. Mechanisms should be in place to know if and when someone accesses the site.
- Require that files containing sensitive data and information are kept in locked file cabinets at all times, other than when an employee is working on the file. Moreover, when an employee is working on the file, make sure that unauthorized people are not able to see the file (e.g., when flying on the plane).
- Remind employees not to leave sensitive documents/information out on desks when away from workstations.
- Require employees to put files away, log off computers, and lock file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to notify if an unfamiliar person is seen on the premises.
- If offsite storage facilities are maintained, limit employee access to those with a legitimate business need. Mechanisms should be in place to know if and when someone accesses the site.
- If devices that collect sensitive information are used, such as PIN pads, secure the equipment to reduce the risk of tampering. Such equipment should also be secured to reduce the risk of an attacker switching equipment with a dummy device.

7.2.7 Protection Levels

Access control (including identity consideration) should be considered at many different levels.

- **Business applications**: applications needed to manage orders, schedule work, organize HR, and finance, etc. Focus is on the protection of sensitive business information and functionalities. Identities usually relate to end users.
- **Operating systems**: base for running applications on laptops, desktops, servers, phones, tablets, etc. Focus is on the protection of files and data, against malware, and what access control can support. Identities usually relate to end users (laptops, phones, etc.) and services (servers).
- **Infrastructure devices and supporting services**: routers, switches, access points, authentication services, etc. Focus is on the protection of correct network traffic, keeping the communication secured, and keeping intruders away. Identities usually relate to technical users and services.
- **Mobile devices**: devices such as phones, tablets, and even laptops. Focus is on the protection of data stored on devices and making sure it is accessible securely to include scenarios like offline usage or theft of device.
- **Premises/physical**: buildings, server rooms, print rooms, offices, workshops, showrooms, etc. Focus is on making sure that people can enter the right places and get access to the right assets.

Moreover, one can map the above to the different network layers:

- Application layer (e.g., HTTP)
- Transport layer (e.g., TCP)
- Internet layer (e.g., IP)
- Network layer (e.g., Ethernet)

It is important make sure that there is full coverage of the IAM in different layers and areas according to the requirements which should be based on information criticality.

- Implement comprehensive protection on all layers and for all types of applications and devices both on physical and logical dimensions.

7.3 Dealership Security Level Maturity Guidance

Dealerships often struggle implementing security recommendations. This is often attributed to the maturity level of the dealership in terms of IT and security sophistication. Use this guide to help identify your dealership maturity level, and the next steps to take to help improve your dealership security posture.

7.3.1 Dealer Guidance on Security Policies

When determining the next steps to mature a dealership's security policies, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have identified and documented policies around acceptable use, audit, access management (including password) and basic network consideration (including external access and wireless standards).
- **Intermediate Maturity Level:** Dealerships have identified and documented policies for all expected areas. Moreover, have processes in place to deliver, educate, and support dealership personnel with documented security policies.
- **Advanced Maturity Level:** Dealerships regularly test, audit, and refine security policies and procedures.

7.3.2 Dealer Guidance on Identity and Access Management (IAM)

When determining the next steps to mature a dealership's IAM, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

Basic Maturity Level

- Explicit processes for managing identities' lifecycle and access rights
- Regular audits and reviews of permissions for critical systems
- Explicit processes for password management
- Basic education of employees (at least for newly hired)
- Access control system for critical physical premises

Intermediate Maturity Level

- Explicit processes for managing identities' lifecycle and access rights
- Regular audits and reviews of permissions for critical systems
- Explicit processes for password management and recommendations on storing passwords on the client side
- Regular education of employees
- Access control system for all physical premises
- Level of protection (e.g., multi-factor authentication, defence in depth) related to the criticality of information and business functions

Advanced Maturity Level

- Automated processes for managing identities' lifecycle and access rights
- Centralized identities' storage and management including right level of identities' federation
- Centralized processes for password management and authentication
- Strong recommendations (or policies) on storing passwords on the client side
- Level of protection (e.g., multi-factor authentication, defence in depth) related to the criticality of information and business functions
- Centralized access control system for all physical premises
- Regular education of employees
- Regular audits and reviews of permissions and identities
- Comprehensive protection on all layers and for all types of applications and devices both on physical and logical dimensions

7.3.3 Dealer Guidance on Patch Management

Basic Maturity Level: Dealerships have each system set to automatically update for critical or security patches.

Intermediate Maturity Level: Dealerships have an enterprise-wide patch management system in place.

Advanced Maturity Level: Dealerships test, rollout, and validate patches as they become available as soon as possible.

7.3.4 Dealership Guidance with Disaster Recovery

When determining the next steps to mature a dealership's disaster recovery/ business continuity, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships regularly back up all systems.
- **Intermediate Maturity Level:** Dealerships perform regular incremental backups and store backup images offsite.
- **Advanced Maturity Level:** Dealerships deploy a business continuity system to include full system backups offsite in a virtual environment that will allow the dealership to spin up the backup image immediately in case of an outage or failure.

7.3.5 Dealer Guidance on Security Awareness Training

When determining the next steps to mature a dealership's security awareness program, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** All employees take annual security training. Training completion is documented, and reporting is available for audit. Employees may be unsure of their role in protecting the organization. Organization may be compliant, but not secure. There is no established process for and/or employees do not feel empowered to report suspicious behavior or accidental data loss.
- **Intermediate Maturity Level:** Training program may be more frequent than annual, and follow-up is conducted to ensure all employees participate as a condition of employment. Topics covered focus on the greatest risks to the organization. Awareness materials are posted in employee break areas. Employees are aware of company security policies and know how to recognize and report a security incident.
- **Advanced Maturity Level:** Training program for all employees and contractors include short but frequent modules on timely topics relevant to their role. Employees are tested on their ability to defend against various social engineer tactics like phishing, USB drops, fraud, etc. Employees know how to report a security incident and when tested, at least 50% of employees report something suspicious. When tested, less than 10% click on phishing test emails. Dealership has a culture of security – employees understand their role in protecting the organization, seek out secure processes, and encourage their coworkers to conduct business in a way that values security and protecting the organization from fraud, theft, and accidental data or financial loss.

7.3.6 Dealer Guidance on Compliance with Federal Legislations

When determining the next steps to mature a dealership's compliance with security legislations, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have researched PCI and GLBA to determine compliance with federal legislation. Dealers have documented policies and processes to meet compliance.
- **Intermediate Maturity Level:** Dealerships regularly review and revise compliance with federal security legislation
- **Advanced Maturity Level:** Dealers perform regular audits on systems and track results back to legislation requirements.

7.3.7 Dealer Guidance on Network Security

When determining the next steps to mature a dealership's network security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have developed and documented an internet usage policy. Dealerships have protection at the network gateway and have configured and segmented the network to avoid unwanted access to network resources. The network is monitored by security information event management technologies in real-time to protect against unwanted network access. Remote access is monitored and restricted on the network.
- **Intermediate Maturity Level:** Dealerships have used documented policies and processes to set up a secure, segmented dealership network. Dealerships regularly test the network against known risks. The network is monitored 24x7x365 by security experts using security information event management technologies. Remote access monitored and restricted to known vendors and employees.
- **Advanced Maturity Level:** Dealerships have used documented policies and processes to set up a secure, segmented dealership network. Dealerships regularly test the network against known risks. The network is monitored 24x7x365 by a SOC 2 certified service provider. The network is monitored 24x7x365 by security experts. Remote access monitored and restricted to known vendors and employees. Employee VPN access is achieved by two-factor authentication.

7.3.8 Guidance with Dealership Antivirus

When determining the next steps to mature a dealership's AV security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have identified all systems and applied antivirus software to each system on the network.
- **Intermediate Maturity Level:** Dealerships have an enterprise antivirus system in place. This includes enterprise-wide license management, an enterprise portal for reporting and response, and audit and reporting across the entire network.
- **Advanced Maturity Level:** Dealers perform proactive, immediate response to alerts generated by the corporate AV solution.

7.3.9 Dealer Guidance on Email Security

When determining the next steps to mature a dealership's email security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships have taken steps to implement technologies to protect dealer email systems.
- **Intermediate Maturity Level:** Dealers perform active inbound and outbound email security inspection and protection. Dealers encrypt sensitive data through email.
- **Advanced Maturity Level:** Dealerships have active email monitoring and response to email threats.

7.3.10 Guidance with UTM/Firewall/IDS

When determining the next steps to mature a dealership's unified threat management, firewall, and intrusion detection system, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships deploy a fully managed and licensed UTM which includes licensing for AV, SPAM, and IDS/IPS. Signatures are automatically updated in real-time.
- **Intermediate Maturity Level:** Dealerships respond to alerts and events from the UTM 24x7x365 in real-time. Dealerships utilize a SIEM (see section 3.5) to alert and respond to events at the network gateway.
- **Advanced Maturity Level:** Dealerships turn to a managed security service provider (MSSP) for proactive, 24x7x365 UTM management, monitoring, and response.

7.3.11 Guidance with SIEM

When determining the next steps to mature a dealership's security information event management, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

- **Basic Maturity Level:** Dealerships install and utilize SIEM software. All alerts are responded to in near real-time 24x7x365. All system logs are stored in accordance with federal legislation (see section 2.6 on compliance with federal legislations).
- **Intermediate Maturity Level**: Dealerships utilize a managed security service provider for advanced monitoring and response. Dealerships integration threat intelligence for advanced monitoring and alerting.
- **Advanced Maturity Level:** Dealerships turn to a SOC 2 certified managed security service provider (MSSP) for proactive, 24x7x365 UTM management, monitoring, and response. Dealerships integrate threat intelligence into the SIEM solution. Tickets, alerts, and activity is regularly reviewed by dealership management and MSSP for security posture refinement, documentation, and improvement.

7.3.12 Dealer Guidance on Application Security

When determining the next steps to mature a dealership's application security, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

Basic Maturity Level

- Introduce an application catalogue.
- Maintain basic identity and access management.
- Apply application updates and patches on a regular basis.

Intermediate Maturity Level

- Maintain application catalogue with understanding of business impact analysis and information classification.
- Implementation of mature identity and access management strategy.
- Protection of information flows from the end-to-end perspective both in transit and storage.
- Introduce processes for handling incidents and access requests.
- Apply defence in depth strategy.

Advanced Maturity Level

- Apply all items from the previous section.

7.3.13 Dealer Guidance on Mobility

When determining the next steps to mature a dealership's security in mobility, first identify the dealership's current maturity level. Next, determine the actions that can be taken to advance the dealership's security posture. Use the guide below to assist.

Basic Maturity Level

- Keep updated antimalware software.
- Define what information can be processed and stored on the mobile devices; include considerations related to managed and unmanaged devices.
- Access to devices should be restricted, requiring user authentication. Most devices can be locked with a screen lock, password, or PIN.
- Update the mobile OS with security patches. Information on patch management can be found in section 2.6.3.

Intermediate Maturity Level

- All items from Basic Maturity Level.
- Apply encryption of data both on laptops and mobile devices with special care of key management for decryption.
- Review all connectivity methods, be careful with automated wireless connectivity since passwords may be exposed as well as a man-in-the-middle attack can be executed.
- Create policies and procedures on who, when, and how to remotely access the company environment (network, servers, applications, etc.) and which parts of it. Deploy appropriate technical solution to support established approach.

Advanced Maturity Level

- Apply all items from the previous sections.

8. 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: **https://www.ctia.org/the-wireless-industry/industry-commitments/app-content-classification-ratings-guidelines**

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 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 a desktop computer 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).

Multi-Factor Authentication (MFA): A security measure, process, or technology that requires users to provide more than one credential to access. Users are generally required to provide a combination of something they know (like a password, Q&A, or PIN), something they have (like a smartphone or USB key), and/or something they are (like a fingerprint or facial recognition)

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. STAR 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 an IEEE 802.11x wireless local area network. SSIDs must be associated with a specific VLAN.

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.

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 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.

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 being connected to the device.