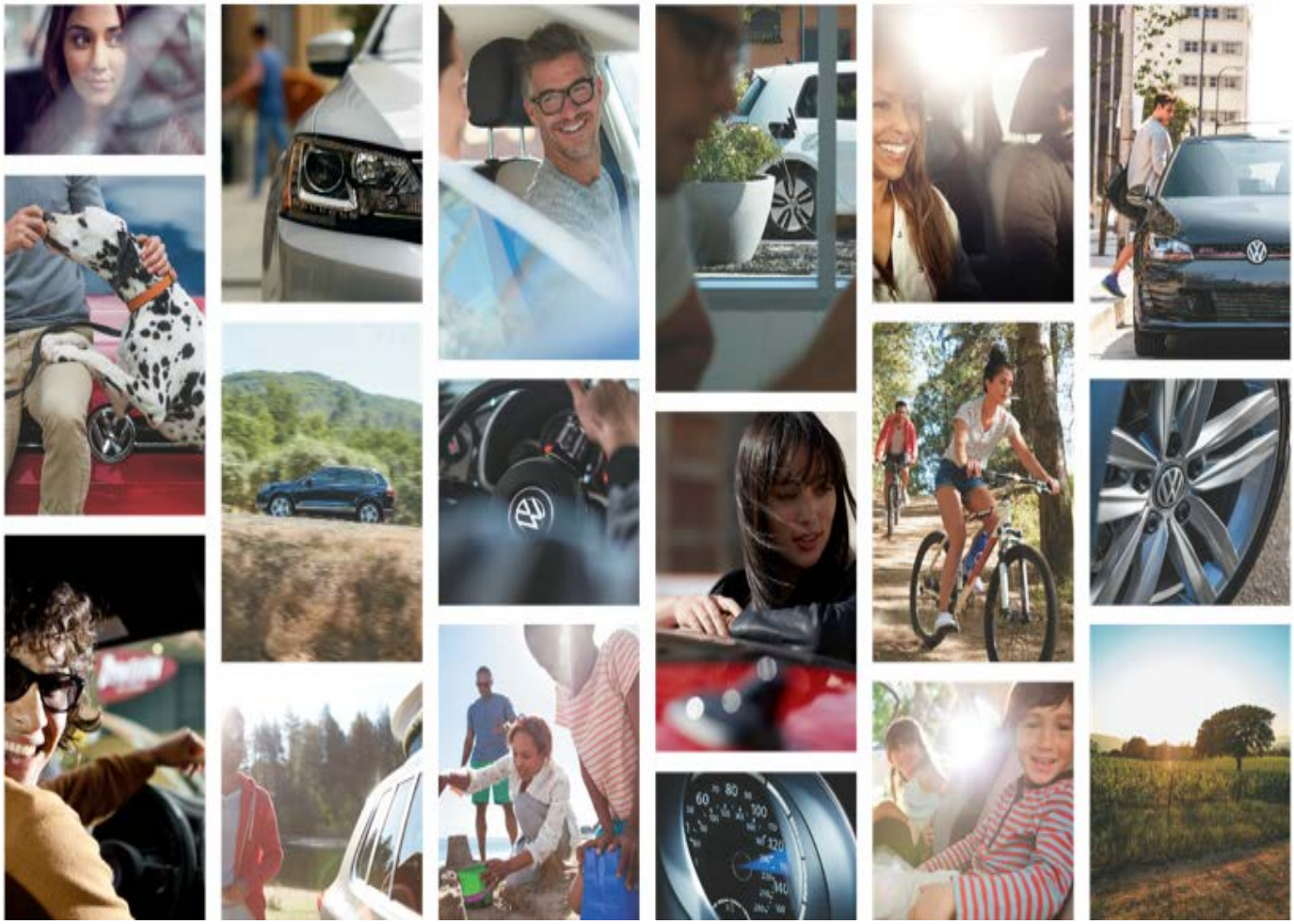


VW Dealer Digital Readiness Standards *2016*

Volkswagen






1| Introduction

1.1 Purpose

Digital Readiness plays a crucial role in preparing dealerships for a heavily IT-driven business that enables a seamless customer experience. Volkswagen of America (VWoA) is thus providing infrastructure recommendations about the business-to-business communication requirements to both dealership and retail technology partners.

The goal of these Dealer Digital Readiness Standards is to ensure that all VWoA dealer partners understand their specific IT requirements, and what our recommendations are for upcoming infrastructure investments – in case a dealer is looking into a component upgrade, contract renewal, remodeling or even new construction of a facility – to meet changing demands cost-effectively while ensuring both top performance and security.

1.2 Benefits of Common Standards

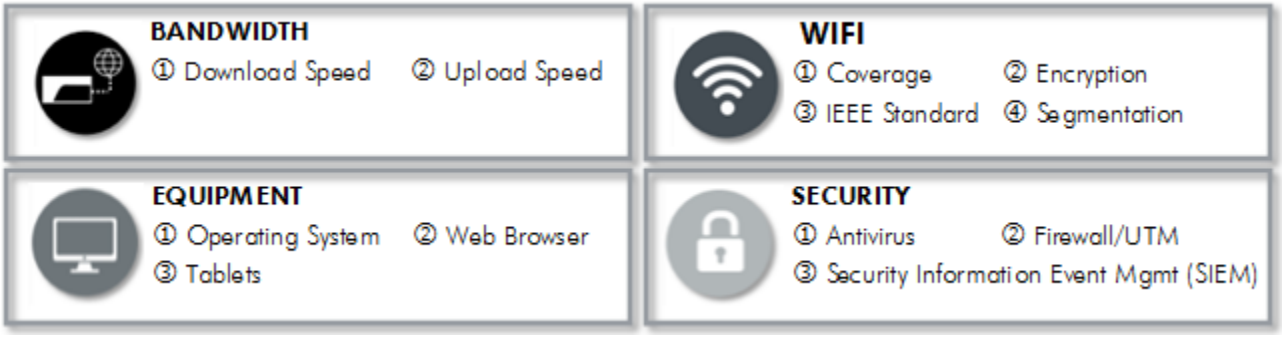
Benefits for dealers are numerous, ranging from the migration to internet-based applications to the use of common standards across original equipment manufacturers (OEMs).

Many of them, however, depend on a having a business-class internet connection and good standards-based network design. Dealers are encouraged to review their internet connection as well as the overall network design in order to maximize the following benefits:

- Better understanding of and more control over your network design.
- Ability to select from a larger pool of technology vendors.
- Long-term reduction in network complexity.
- Potentially lower cost through reduced complexity and redundancy.
- Allowed access to web-based applications and mobile devices.
- Use of open standards — not dedicated-OEM infrastructure, but flexible internet infrastructure that is open to other OEMs and consistent with the National Automobile Dealers Association (NADA).
- Leverage speed of new application upgrades and deployment.
- Enabled dealership personnel to access any application from any device in the dealership.
- Facilitated data sharing within the dealership.
- Enabled public internet access from all points of the dealership.
- Increased security against intrusion or infection.
- Increased stability with customers using the dealerships' public wifi network.

2| Digital Readiness

Digital Readiness relates to the following areas of the dealer IT landscape:








The standard in each area is listed in the following table:

	✓ Minimum	✓ Recommended
BANDWIDTH		
① Download Speeds ② Upload Speeds	1 - 20 users: 25 Mbps download, 10 Mbps upload 21- 60 users: 25 Mbps download, 25 Mbps upload 61 + users: 50 Mbps download, 25 Mbps upload	1 - 20 users: 25 Mbps download, 25 Mbps upload 21- 60 users: 50 Mbps download, 25 Mbps upload 61 + users: 75 Mbps download, 25 Mbps upload
WIFI		
① Coverage	Business Access: 1) Sales Showroom, 2) Service Drive, 3) Service Shop & 4) All customer waiting areas/lounges Guest Access: 1) All customer waiting areas/lounges	Same as minimum
② Encryption	Business Access: WPA2 Guest Access: WPA2	Same as minimum
③ IEEE Standard	Business Access: 802.11a or 802.11g Guest Access: 802.11a or 802.11g	Business Access: 802.11ac or 802.11n Guest Access: 802.11ac or 802.11n
④ Segmentation	Segmentation via Firewall/UTM, VLAN or Layer 2 Switch **AND** separate network access password for guest vs. dealership employees.	Separate internet connection exists for guest access **AND** separate network access password for guest vs. dealership employees.
EQUIPMENT		
① Operating System	Windows 7	Windows 8 or higher
② Web Browser	IE 11 & Mozilla Firefox	Same as minimum
③ Tablets	Apple iPad /iPad Mini, ≥ iOS 9 (most current version)	Apple iPad Air 2 /iPad Mini 2, ≥ iOS 9 (most current version)
SECURITY		
① Antivirus	Antivirus required to maintain active subscription & automatic signature updates.	Same as minimum
② Firewall/UTM	Firewall/UTM with IPS/IDS required & filters must be used. State-aware firewall capabilities within router sufficient.	Same as minimum
③ SIEM	Recommendation only	Proactive, real-time event monitoring. Ability to collect data & correlate varying security data from the network in real-time. SIEM service provider must be able to notify the network admin in the case of a security event &provide proper documentation for compliance purposes.

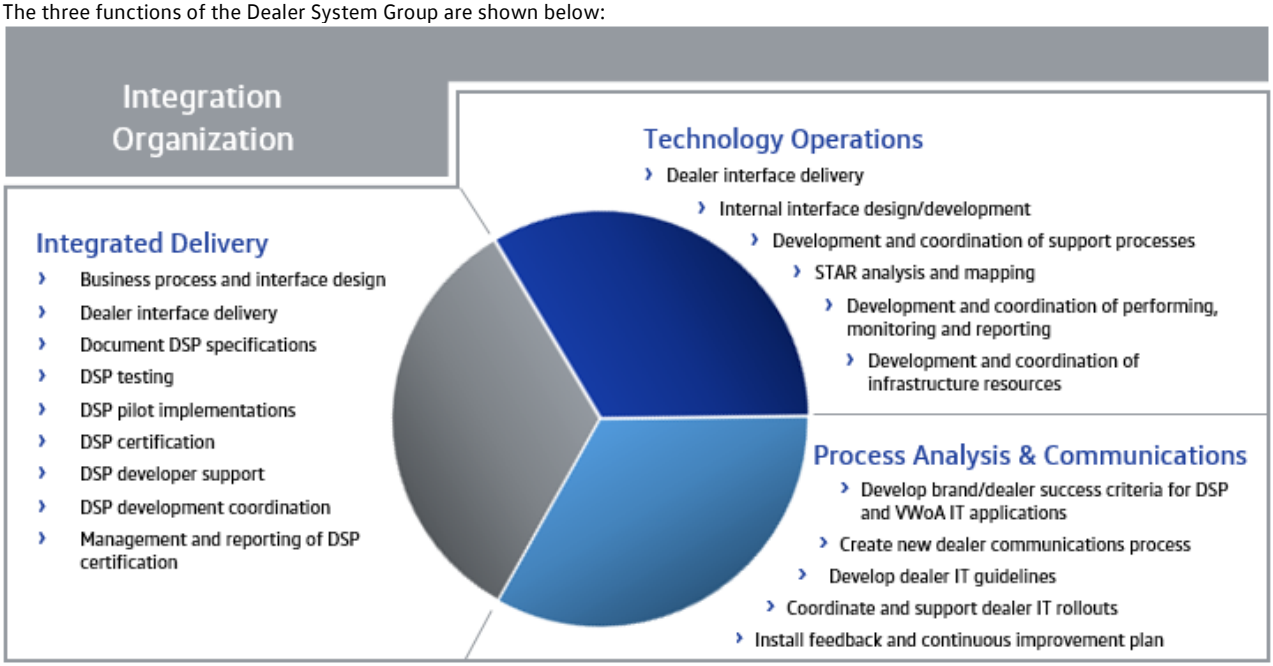
3| Dealer System Group

3.1 Overview & Organizational Structure

In order to focus on the optimization and improvement of factory-to-dealer communications, IT has created a Dealer System Group. This group utilizes current operations and project resources to document and measure the performance of dealer systems support. In addition, this group also works to prioritize and implement new dealership management systems interfaces based upon project and operating needs.

The primary goal of this group is to work with dealerships to establish and exceed satisfaction measurements with regard to dealer systems support and factory-to-dealer integration.

The three functions of the Dealer System Group are shown below:



3.2 Dealership Support & Service

The IT Service Desk is the Single Point of Contact (SPOC) for all dealer IT-related issues. IT Service Desk is available at 1-866-892-3375.
The goal of the IT Service Desk is to validate and resolve as many issues as possible at first contact, thereby eliminating the need to route the call to 2nd-level support teams and reducing the time to resolve incidents.

3.3 Fully Supported Applications

The following applications are fully supported by the IT Service desk. These applications are fully owned and managed by VWGoA. Services will include first-contact resolution when possible, routing of incidents to the appropriate 2nd or 3rd-level application support teams, following incidents to closure, and providing communications and coordination between the dealer and the appropriate support team.

The IT Service Desk model is based on a global process standard called Information Technology Infrastructure Library or ITIL Version 2, along with proven industry best practices in service management. The use of ITIL methods ensures a consistent and repeatable process for incident management.

Application Area	Fully Supported Applications
Certified Pre-Owned	› OMD Web › VCAS (found in
Parts	› Parts on Command
Vehicle Sales	› OMD Web › Checkpoint Reporting System (CRS) › VIN Incentive Search
Service & Warranty	› Elsa Pro › GeKo › GFF Paperless › SAGA/2 › Service Net › Star Tester Support › VAS devices › Warranty Parts Portal (WPP)

3.4 Limited Support Applications

Many dealer-facing applications are not directly owned or managed by VWoA. Some examples include:

- All Academy training applications
- PartsVoice
- DMS applications

These applications are typically managed by external third parties or by VW AG; therefore, the IT service desk has limited access to the necessary support resources. When a call is received for one of these applications, the IT service desk will provide the dealer support contact information for the third-party vendor that manages the application.

3.5 Applications & Program Support Contact List

The following is a partial listing of potential support center contact telephone numbers for dealer employee reference. This information, while updated semi-annually, is subject to change.

IT Service Desk: 1 -866-892-3375

Program	Contact Information
VW Academy - Corporate	866-873-7569
CDK - STAR DMS Integration Support	877-483-9171 Option 2 to reach the ECC
CDK DCS Support	888-418-4464
CDK ETKA	800-811-0957
VCI Dealer Extranet	888-464-2834
AFS Dealer Remarketing	877-557-6824
VW AfterSales Marketing Operations Center (Peak)	888-289-9841
VIM	IT Service Desk
VW Academy (CRC)	crcsupport@vw.com Please contact your Regional Training Coordinator
VW AG - Wolfsburg	011-49-0-1806-890000
VW Analytics	TBD-TBD-1TBD
VW Critical Parts Alert	866-892-3375
Dealer Marketing Center (CDK)	888-778-7048
VW Incentive Portal	IT Service Desk
VW Insight	877-494-1TBD
VW IT Service Desk	866-892-3375
VW Lead Intelligence (ALI/ELS)	888-252-1TBD
VW Service Supplies eStore	IT Service Desk

Program	Contact Information
VW Direct	877-557-6824
Dealer Business Intelligence (DBI)	866-605-9441
ElsaPro	IT Service Desk
GFF Paperless	IT Service Desk
Helpdesk for ODIS Hardware Support	866-328-7004
ODIS	IT Service Desk
Parts on Command Support	800-767-6552
PE Connect	703-636-3652
Product Compliance	800-741-2919
Reynolds & Reynolds DMS Integration Support Desk	800-767-0080
Reynolds & Reynolds ETKA Catalog Helpdesk Support	800-661-8600
ServiceSmarts Online	313-262-3686
Siemens VAS Hardware Support Desk	800-215-1646
X-Time Scheduling System Help & Support Desk	866-605-9441
Stationary Ordering Site	313-624-3300
Technical Help Line - VW	800-388-2834
Technical Literature Ordering Website	800-544-8021
Touch up Paint	800-550-4062

VW Special Tools & Equipment	800-892-9650
VW Standards Management System (SMS)	866-605-9441
Generation VW	Tbd-tbd-1tbd
WPSP	IT Service Desk
TDI	Tbd-tbd-1tbd

DealerTrack DMS Dealer Communications Support	www.dealertrack.com/portal/my-dealertrack-support
Urban Science Help Desk	877-208-8711
Auto/Mate AMPS Dealer Communications Support	877-707-4129
VW DIT Program	248-295-9180

4| Dealer Personnel Setup & Onboarding

4.1 New, Buy/Sell, Terminated Dealer Process

Technical Analysts from IT&S manage the new point, buy/sell, move and termination process for dealers. This includes support to dealers, corporate and field teams for dealer set up in VW Hub and related sites. The figure below represents the steps involved in this process for both Volkswagen of America and the dealership.

Volkswagen Dealer Digital Readiness Program Consultants will support dealers with IT infrastructure related matters during transition. For questions and/or assistance, please contact the Volkswagen Dealer IT Program Consultants at 248 295 9180.

Volkswagen Dealer IT Program: 248 295 9180

Unofficial Dealer Change Notification received from Network Development Teams

Technical Analysts discuss process with Dealer

Technical Analyst sends forms to Dealer

Dealer returns completed forms to appropriate parties

Technical Analysts provide support to Dealer & Field teams during transition

Required Forms

New Point	Buy/Sell	Termination
› Dealer Communication Memo › Extranet Administrator Request Form › BeKo Informational Letter › BeKo Certificate Maintenance Form › BeKo User ID Request Form › ETKA Agreement › CES Agreement › D2D Data Extraction Form › D2D FAQ's Document › 3-Digit ID Informational Document › STAR Connect Form › PBB Form › Volkswagen DBI Form	› Dealer Communication Memo › Extranet Administrator Request Form › List of Employees to Transfer › New Employee Add Form for Certification Resource Center › CES Agreement › D2D Data Extraction Form › D2D FAQ's Document › 3-Digit ID Informational Document › Star Connect Form › PBB Form › Volkswagen DBI Form › Temporary ID Form	› Temporary ID Form

4.2 VW Hub Unified Dealer Extranet (UDE) Overview

VWHub.com is the Volkswagen of America enterprise dealer portal that provides a centralized, full-service starting point that allows VWoA to promote, deploy, and manage a broad range of applications, services, and content to our dealer network. VW Hub provides a secure environment for content and connect to applications through Single SignOn.

4.2.1 VW Hub Roles & Security

There are three primary extranet security roles within Volkswagen of America: Dealer Admin, Dealer General, and Dealer GM/Principals. Below is a short description of the two primary dealer roles.

Dealer Extranet Administrator	Dealership Departmental Users
Extranet administrators have the ability to add, modify and delete dealership employee accounts within the UDE, VW Hubportal.com. Particular business applications within VW Hub are accessible only to select roles or personnel. The extranet administrator is tasked with the verification of these requests with dealership management depending on the nature of the request and the requester.	Dealership departmental users have access to VW Hubportal.com and business applications that are used every day to perform their jobs. To login to the extranet, each employee must register for an account. The extranet administrator will create an initial account in the extranet, and then the employee will complete the online registration to obtain the account. Creation of the account itself can happen immediately, however, access to third-party sites must be granted by the extranet administrator.

4.2.2 VW Hub (www.VWHub.com) User Administration

The Volkswagen UDE site, VW Hub (www.VWHub.com), includes detailed instructions on system administration including topics such as adding, finding, deleting and disabling users. This information is easily accessible through the VW Hub Help Center.

4.2.3 Business Application Access Request

Access to certain sites or systems within VW Hub require additional permission. The Request Site Access page is used to send a request to the extranet administrator for each of these systems that require additional permission. Each request is approved or denied based upon the management policies of the dealership.

Instructions for setting up dealer employee access can be found by clicking the help link on the extranet home page.
VW Hubportal.com Access Request Page: VW Hub > My Account > Administration > Access Request

4.2.4 Dealer Employee Setup/On-boarding Recommendations

Item	Minimum	Recommended
Extranet Administrator	2 Training Extranet Administrators	3 Trained Extranet Administrators
Active VW Hub User ID	No lapsed VW Hub user ID's	No lapsed VW Hub user ID's
User ID Deactivation*	≤24 hours from separation of employment	Immediately on separation of employment

***IMPORTANT NOTE: As www.vwhub.com dealer extranet is accessible from the public internet with an active ID and password, terminated dealership employees are able to access systems and applications until their profile is deleted. In order to mitigate security risks, if is VERY IMPORTANT that Dealer Extranet Admins DELETE User IDs quickly after ALL employee terminations.**

5| Dealership Infrastructure Guidelines

5.1 Overview

This handbook has been created to provide dealer employees, DMS providers and local IT support firms with detailed reference material for use when configuring local hardware, software, networks and data integration.

If followed, these guidelines should create the best and most optimized IT systems when working with the Volkswagen brand. The following sections provide general local hardware, software, networking, internet and data security guidelines for use by your DMS and IT providers when configuring or modifying current dealership infrastructures.

For any questions regarding Dealer IT Infrastructure Guidelines, please contact the Volkswagen Dealer IT Program Consultants at 248 295 9180.

Volkswagen Dealer IT Program: 248 295 9180






5.2 Hardware

Client hardware in the dealership is the responsibility of each individual dealer. VWoA establishes the minimum specifications necessary to run essential applications and systems.

5.2.1 Hardware Device Recommendations

Item	Minimum	Recommended
Operating System	▪ Windows PC ▪ Windows 7	▪ Windows PC ▪ Windows 8 or higher
Browser	Microsoft IE 11 and Firefox	Microsoft IE 11 and Firefox
Monitor	17″ LCD Display 1280x768 resolution	24″ LCD Display 1920x1080 resolution
Refresh Policy	Every 4 years	Every 3 years
Anti-Virus Policy	Maintain active subscription and automatic signature updates	Maintain active subscription and automatic signature updates
Tablet	▪ Apple iPad / iPad mini ▪ ≥ iOS 9 (most up-to-date version)	▪ Apple iPad Air 2 / iPad mini 2 or 4 ▪ ≥ iOS 9 (most up-to-date version)
UPS	Suitably sized UPS for on premise servers	Suitably sized UPS for on premise servers and VOIP phone systems
Recovery System	Disaster recovery for any locally maintained systems	Daily, full backups and virtual disaster recovery (DR) capabilities

5.2.2 Tablets

Tablets are handheld devices designed for mobility and accessibility. Many tablets do not 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 calls for higher mobility and accessibility. Tablets should only be used with Volkswagen applications designed for tablet environments. When selecting a tablet device for use with Volkswagen applications, use only the tablet recommended for that specific Volkswagen application.

5.3 Standardizing

A tremendous amount of time and effort can be saved by standardizing the equipment and software utilized by the dealership. This means that the majority, if not all, PCs in the dealership should be built on the same hardware and software platforms. Adopting this practice will streamline deployment and simplify training and support for users and staff.

5.4 Workstation and Internet Access Layout

The minimum acceptable functions and workstation counts for VWoA are:

- Sales Computer Terminals: 1 for every VW Sales Associate
- Technician Computer Terminals: 1 for every 2 Certified Technicians
- Volkswagen Service Advisor: 1 for every Volkswagen Service Advisor
- Parts Department: 1 terminal with ETKA at Retail Counter and 1 terminal with ETKA at Service Counter
- Warranty Administrator: 1 dedicated terminal for every Warranty Administrator






5.5 Networks

The primary advantage of upgrading the dealership's network infrastructure is to reduce the complexity and cost of supporting proprietary solutions previously required for each of the dealer's franchises. Consolidating the network infrastructure can contribute to the reduction of equipment requirements, maintenance responsibilities and related expenses.

Recommendations are given to ensure all equipment is reliable, upgradeable and scalable. Overall, flexibility of the network is necessary to accommodate changing and emerging technologies, as well as to allow open integration with other OEMs.

5.5.1 Network Architecture

The network must be Ethernet-based supporting 100BaseT and/or 1000BaseT or higher. Keep in mind that slower links in key parts of the network may create bottlenecks. The dealer is expected to build an Ethernet LAN according to industry standards associated with the type of cabling used (i.e. Category 5, 5e, 6 etc.). VWoA strongly recommends that this LAN have a central wiring repository where all cable runs are terminated on patch panels.

It is strongly recommended that wiring switches, routers, firewalls and communications equipment are located in a secure room and that all equipment is securely mounted on racks or shelves.

Precautions are required to protect this equipment from damage due to poor power conditions and changes in temperature and humidity.

5.5.2 Network Infrastructure Recommendation

Item	Description
Local Area Network	Ethernet based
Speed	Minimum Fast Ethernet (100BaseT or higher). Gigabit Ethernet (1000BaseT or higher) for new installs.
Wiring	Minimum Category 5 standards. Category 5E or 6 for new installations. Note that if 10 gigabit Ethernet is used, category 6a or 7 is required. Fiber optics cable used inside on long runs (over 295 feet) and between buildings where possible. Wireless methods can be used (with caution) where wired options are not possible or too expensive. New wireless equipment should meet 802.11n or 802.11ac standards.

5.6 High-Speed Internet Access (HSIA) Recommendations

Dealer Size	Minimum	Recommended
1-20 users	25Mpbs download, 10Mbps upload	25Mpbs download, 25Mbps upload
21-60 users	25Mpbs download, 25Mbps upload	50Mpbs download, 25Mbps upload
61 + users	50Mpbs download, 25Mbps upload	75Mpbs download, 25Mbps upload
Item	**Minimum**	**Recommended**
Internet Outage Back-up	3G/4G mobile broadband backup / failover capability	Dedicated backup / failover capability to secondary internet connection, with adequate bandwidth to support normal business functions.

A user being an employee who has full-time access to one or more devices that connect to the internet such as PCs, laptops, tablets etc. Internet download and upload speeds dedicated solely for Volkswagen Dealer employee users and Volkswagen applications. For any third-party online applications used (such as CRM tools, streaming media, online backups, etc.) please check the vendor's bandwidth requirements.

5.7 Wireless Network

Wireless LANs enable network communication and connectivity without the physical restraints of hard-wired cabling. Wireless technology can be especially useful in building-to-building communication or connecting laptops, printers or other wireless-capable items such as tablets to a network where wired cabling is difficult or expensive.

5.7.1 Wireless Network Recommendations

Minimum	Recommended
Dealer MUST ensure via use of separate SSIDs, VLANS, firewall policies, etc., that absolutely no communication can take place between public and business networks. Business and Public networks must be password protected separately. Business and Public networks must be secured with WPA2. Public (guest) access must be made available in all customer waiting areas/lounges; availability must be disclosed. Business access must be made available in the following areas: Sales Showroom, Service Shop, Service Drive and All customer waiting areas/lounges. Guest wireless should have policies in place to limit bandwidth use. This will prevent guest access from interfering with business operations by consuming too much bandwidth. Strong wireless coverage in the 5 GHz and 2.4 GHz band will be required for Business access in the service bay. IEEE Standard: 802.11a or 802.11g	A separate internet connection can be dedicated for public (guest) access. Appropriate web filtering policies should be in place to prevent inappropriate use. The dedicated guest internet connection can also be used as a backup internet connection in case the primary one fails. Business and Public networks must be password protected separately. Business and Public networks must be secured with WPA2. IEEE Standard: 802.11n or 802.11ac

5.7.2 Wireless Deployment Recommendations

Existing wireless infrastructure should, at a minimum, use 802.11a or 802.11g standards. Note, 802.11ac or 802.11n standards are recommended and should be used for new deployments or planned upgrades. All standards are backward compatible, but keep in mind that many devices only support the 2.4 GHz band. Deploying dual band access points is highly recommended. Wireless access points should be enterprise class hardware from a reputable vendor. For example, the Cisco Aironet 1600 series or equivalent. Note that bandwidths shown below are theoretical maximum speeds. In practice approximately 40-50% of that value is achievable.

All wireless deployments should begin with a professional site survey. By conducting the site survey, the wireless vendor will be able to determine:

- Relative density of wireless client devices in different areas of the dealership
- Required areas of coverage (Potential expansion to service drive in the future)
- Potential sources of interference and competing wireless signals
- Structures or objects that may block signals
- Appropriate access point mounting methods away from sources of interference
- Placement of individual access points, taking into consideration channel overlap, coverage and throughput requirements

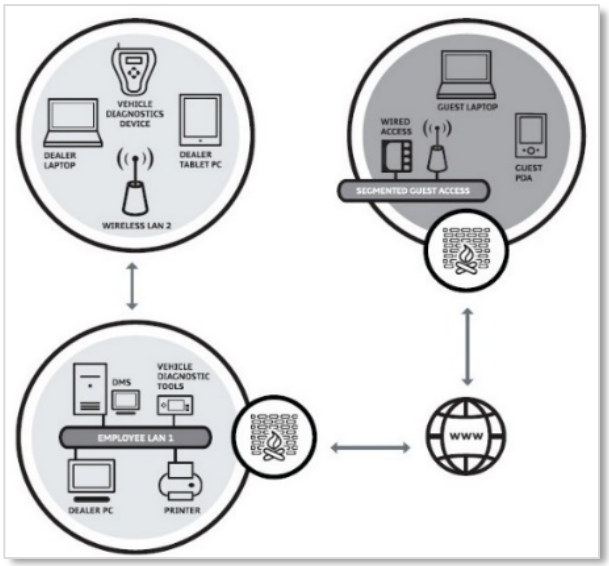
All of this information is required to achieve a uniformly fast and reliable wireless network.

802.11 Standard	2.4 GHz Throughput	5 GHz Throughput
802.11b	11 Mbit/s	N/A
802.11g	54 Mbit/s	N/A
802.11a	N/A	54 Mbit/s
802.11n	150 Mbit/s	300 to 450 Mbit/s
802.11ac	N/A	From 433 Mbit/sec up to multiple Gbit/sec

5.7.3 Wireless Vehicle Diagnostics (ODIS)

- Strong wireless coverage in the service bay in the 5 GHz as well as 2.4 GHz band
- 802.11n/ac standards or higher
- Site Survey may be required to get desired coverage
- Plan for wireless bandwidth. Each VAS diagnostic tester can use up to 7.5 Mbit/s of wireless bandwidth while in use.

Access Point



5.8 Wireless Security

The need for security on any network is paramount, even more so with wireless networks. Typical wired networks have a degree of security inherent in them because physical access is limited by the confines of a building structure.

Wireless networks, on the other hand, are more vulnerable because data is transmitted through the air, making access possible from anyone within range of the wireless access point. A comprehensive security solution can be achieved through the following:

- Encryption (e.g. WPA2)
- Authentication (e.g. EAP-PEAP, EAP-TLS)
- Firewalls/UTM
- Media Access Controller (MAC) address filtering
- Changing the default settings

5.8.1 Wireless Security Options

There are multiple standards when it comes to wireless encryption. The three main formats are WPA, WPA2 and WEP. Previously WEP was the industry standard; however, it has been found to have serious flaws, leading to the development of WPA and WPA2. WPA2 is a stronger and more effective standard. WPA2 is the minimum requirement and it is strongly recommended that all security settings be updated to utilize WPA2. Note: some legacy devices may not be able to update to WPA or WPA2.

5.9 Security Recommendations

Topic	Description
Firewall/UTM	Filters MUST be used. State-aware firewall capabilities within a router may be sufficient.
Personal Firewall Software	MUST be used on any machine that is mobile. Should be used on every PC in the dealership.
DMZ	Recommended for any network device or service that needs to be accessed from the public internet.
Web/URL filtering	Recommended for controlling outbound internet access and URL filtering.
Virtual Private Network (VPN)	Not required at this time, but recommended by VWoA as some OEMs may require this in the future for a secure two-way communication. Recommended for wireless LAN segments to protect data from unauthorized eavesdropping.
Intrusion Detection/Prevention Software (IDS/IPS)	Should at minimum be implemented at the network edge with regular subscription signature updates
SIEM (Security Incident and Event Management)	Security Information and Event Management: Proactive, real-time event monitoring that utilizes a SIEM (Security Information and Event Management) service. 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.
Antivirus Software	MUST be used with regular automatic signature updates. Software should be used on all firewalls, servers and clients to help prevent damage to dealership data.
Wireless LAN	Recommend WPA2 Enterprise for the business wireless network. This includes both encryption and authentication. ****NOTE:** WEP is very insecure and should not be used.

5.10 Local Area Network (LAN) Recommendations

A robust and reliable LAN is essential to conducting business in the dealership. A network that is not functioning well can cause a loss of productivity and severe disruptions to business in all areas of the dealership.

5.10.1 Voice over IP (VoIP)

Before deploying a VoIP system, consult the vendor about requirements to ensure your network hardware supports the necessary features. Without the proper Quality of Service features, call quality may be poor and unreliable. These features will likely include:

- Virtual LANs (VLAN)
- 802.1Q trunks
- DiffServ QoS
- Class of Service (CoS)
- Power over Ethernet (PoE)

5.11 Connection to VWoA

As part of open STAR-based standards, dealers will be able to fully connect to VWoA systems and applications from an open internet connection. Dealerships must maintain a secure and high-speed internet connection in order to utilize VWoA systems and applications adequately. VWoA reserves the right to deny access to dealerships and individuals regardless of connection type.

5.12 Connection to applications hosted at VWoA, VW Group & 3rd parties

Similarly to above, a secure and high-speed internet connection will enable dealers to access all VWoA systems and applications including third-party applications and VW AG hosted systems and databases. Access to these systems are managed and maintained solely by VWoA dealer extranet administrators on behalf of their dealerships. VWoA reserves the right to deny access to dealerships and individuals regardless of connection type.

5.13 Virtual Local Area Network (VLAN)

A Virtual Local Area Network (VLAN) (IEEE 802.1Q Virtual LANs) should be considered in environments where users are required to access applications and data from dissimilar networks, such as a dealership LAN, DMS LAN, OEM 1 LAN, OEM 2 LAN, etc.

VWoA encourages dealers to adhere to OEMs recommendations for integrating multiple LANs that require different IP addressing using a router and an Ethernet switch that fully supports IEEE 802.1Q VLANs.

5.14 Data Cabling

For existing installations, all connectivity products (this includes copper cable, jacks, inserts, modular plugs, patch panels, patch cords, etc.) must meet or exceed TIA-568-A Category 5e standards. Though this section references TIA-568-A category 5 and 5e standards, when the majority of the dealership's cabling is scheduled for replacement, Category 6 cabling is recommended. Note that 10 gigabit Ethernet requires Category 6a or 7 cabling. While this speed is very seldom used to connect workstations, it may occasionally be used for links between network devices or for higher performance servers.

Installation must be performed by certified installers and done in accordance with TIA-568-A Category 5 standards. No horizontal cable runs should exceed 90 meters (295 feet). Cable runs must not be installed near or parallel to anything that may produce electromagnetic interference (EMI), such as fluorescent lights, electric motors, etc. It is also suggested that a few feet of "service loop" is left for future serviceability, moves, additions and changes.

All cables and jacks (wall and punch panel) must be labeled clearly. The main distribution frame/intermediate distribution frame (MDF/IDF) end of each cable run should be terminated on a Category 5E or 6 patch panel or an organized jack/insert system. The workstation end of each cable run must terminate on a Category 5e or greater 8-position jack. All terminations must be compliant with TIA-568-B wiring configurations.

All interconnections and cross-connections must be made using at least Category 5e. Lengths of said patch cords should comply with the appropriate TIA-568-A standard for the category of cable used. Copper Ethernet cable should not be used outside of buildings or to connect multiple buildings. In this case, fiber optic cable or wireless connections are viable alternatives.

5.14.1 Fiber Optic Cabling

Fiber optic cable is highly recommended in place of data cable runs when the length exceeds 295 feet in a campus environment or when connecting buildings together with right of way allowed. A minimum of four strands of multi-mode 62.5/125 microns is required. Extended distances or the implementation of gigabit Ethernet may require the use of single-mode fiber optic cabling. The environment in which the cable is installed will determine the type of jacket it requires. Plastic flexible tubing should be used when installing fiber optic cable if conduit is not available.

All cabling must be dressed into the MDF/IDF in a secure manner, which restricts movement. Terminations should be made with standard ST, SC or LC style connectors. Cables should terminate at a fiber patch panel. Fiber optic patch cords should be used to connect the patch panel to the Ethernet switch or other device. Fiber-to-copper media converters may also be needed.

5.15 Building Codes

All local, state and federal building, fire and safety codes, rules, regulations, statutes and laws must be strictly adhered to. Plenum-rated cable must be used in all areas where required. These codes may also require that cable runs may not touch or be fixed to anything that is not part of the permanent structure, such as drop-ceiling grids and electrical conduit.

All installed drops must be tested and certified. All cables tested must pass in accordance with TSB-67, TSB-95 and Category 5e (or better) guidelines. An electronic copy as well as a certified printout of the test results signed by the technician should be requested by the customer contact.

5.16 LAN/WAN Hardware and Configuration

A robust and reliable LAN/WAN is essential to conducting business in the dealership. The below sections offer recommendations for LAN/WAN hardware selections and configurations.

5.16.1 Switches

Ethernet Switches are used to connect computers and other network devices together. Switches are also used to logically separate different subnets into VLANS (virtual LANs) Below are some guidelines for selecting this equipment:

- Devices must match the IEEE 802.3 specification for Ethernet.
- Connection of multiple switches together should use redundant links of the highest speed available, using STP or rSTP to ensure a loop-free topology.
- For very busy networks, multiple ports can be used for a single logical uplink between switches using link aggregation or Etherchannel. This provides redundancy as well as greater speeds.
- Devices with redundant power supplies are recommended to help minimize potential downtime.
- Devices should be stackable or rack-mount style for neat, safe and uniform installation.
- Switches with VLAN and 802.1Q trunk technology should be used for routed networks with multiple subnets or VLANs.
- Managed devices should support industry remote management standards such as Simple Network Management Protocol (SNMP) and Remote Network Monitoring (RMON).
- 100 or 1000 Mbps or higher devices should be used.

5.16.2 Routers and Firewall

Routers allow computers from different networks and subnets to communicate. In dealerships, routers may be used to connect an OEM LAN, dealership LAN and DMS LAN to the internet. In most cases a firewall can be used for these functions. Listed below are some general guidelines for selecting this equipment:

- Devices must have at least two 100 or 1000baseT Ethernet interfaces (LAN and WAN). Additional Ethernet interfaces may be required.
- Devices used as for internet links should have enough interfaces to add a backup internet link.
- Devices should have expansion modules available to allow connection to other devices such as Digital Signal X (DS1) for Private Branch Exchange (PBX) for IP Telephony internet.
- When connecting two or more LANs, the router or firewall should support 802.1Q trunks to allow multiple VLANs on a single Ethernet interface.
- Routers and Firewalls should support dynamic routing using RIPv2, OSPF and BGP.
- Routers and Firewalls should support Network Address Translation/Process Analytical Technology (NAT/PAT).
- Routers should support Dynamic Host Configuration Protocol (DHCP) as a server and a client.
- Firewalls and routers with integrated firewalls should have Next-Gen firewall functions such as IDS/IPS, Content Filtering, and Antivirus.
- Most ISPs today offer an Ethernet handoff for their internet connections so specialized interfaces are usually not necessary. However, it is best to buy a modular router in case a special interface card is required at any time.
- Routers and Firewalls should support remote management protocols such as SNMP, Netflow, sFlow, etc.

Router and Firewall Setup and Configuration

Configuration varies from one brand of equipment and another. It is best to have a professional technician handle the configuration and management. Listed below are basic guidelines for setup and configuration of this equipment:

- Change the default password. More often than not equipment manufacturers use the same default password in all of their products.
- Ask for a copy of the configuration file on disk. If for some reason the router has to be replaced, having a copy of the latest configuration files on disk can save time and significant money.
- Insist on labeling each interface and cable. This will save time when tracing back cables and acts as a self-documenting process others can follow.
- Secure the router in a rack or on a shelf. Take the time to mount the device securely. Preferably, this should be in a rack with other communications gear.

5.16.3 Ethernet Network Interface Cards

Any device connected to an Ethernet LAN must have an Ethernet card. The guidelines that follow are valid for all Ethernet cards, regardless of whether they are integrated into the main system board or installed separately. General guidelines for purchasing an Ethernet card:

- Devices to be used must match the IEEE 802.3 specification for 100baseT and 1000baseT.
- 1000 Mbps NICs are recommended.
- NICs must have a RJ45 interface for a twisted-pair connection.
- Onboard light-emitting diode (LED) status indicators to allow for easier troubleshooting of connection problems.
- Wireless NICs should be IEEE 802.11a/b/g/n compatible and support and support dual band (2.4 and 5 Ghz).
- Certification of interface cards by the operating system suppliers is highly recommended.

5.16.4 Equipment Certification

All equipment should be a brand produced by a reputable manufacturer with a history of quality merchandise. All equipment should be accredited or certified by one or more of the following organizations and agencies:

- UL - Underwriters Laboratory
- CSA - Canadian Standards Association
- ISO - International Standards Organization
- IEEE -Institute of Electrical and Electronic Engineers
- CCITT - Committee to Consult on International Telegraph and Telephone
- ITU - International Telecommunications Union

5.16.5 Controlled Environment/Equipment Care

A controlled environment is necessary for LAN equipment. Most service providers require a controlled environment as a condition for honoring warranty claims or service contracts. OEMs recommend the following guidelines to maintain the equipment and help prevent network outages:

- Do not stack equipment in a way that prevents heat dissipation or contrary to manufacturer recommendations.
- Do not block cooling fans.
- Do not place equipment in dusty environments.
- Do not place equipment or run wiring near anything that generates vibrations or strong electromagnetic fields (e.g., air conditioners, welders, transformers, etc.).
- Do not switch devices off and then on rapidly. Wait 10 seconds before turning something back on.
- LAN equipment should be installed in a secure area that provides controlled temperature and humidity.
- Routers, switches and other LAN devices should be installed on a Category 5-compliant rack or cabinet within close proximity to the horizontal cabling system.
- Racks should be anchored to the floor or mounted to a wall in a secure fashion per manufacturer's specifications.
- A wire management system should be used to keep the cross connections of all devices neat and serviceable.
- All equipment, ports, jacks and wiring should be properly labeled.
- All AC electrical outlets should be connected to dedicated circuits. Qualified licensed electricians must perform electrical work.

5.17 Domain Name Service (DNS)

The Domain Name Service (DNS) is an internet directory service used to translate readable domain names (e.g. *Volkswagen-vw.autorepair.com*) and internet Protocol (IP) addresses (e.g. 192.168.45.230). Volkswagen of America recommends exclusive use of public DNS, unless utilizing Microsoft Active Directory (AD).

5.18 Network Services Recommendations

Element	Description
Addressing	ISP should provide routable public IP addressing. Use dynamically assigned private addressing for devices on the LAN.
Routing	Have a professional handle routing configuration. Change and protect passwords for routers. Save backup configurations to CD or USB drive. Label router and wiring properly. Mount router securely in a rack.
Routing Hardware	Consider current needs and allow for future expandability when selecting routers and feature sets.
Dynamic Host Configuration Protocol (DHCP)	DHCP should be used to simplify network configuration and administration.
Domain Name Service (DNS)	The exclusive use of public DNS is recommended except when using Windows Active Directory, in which case having an internal DNS server is required.

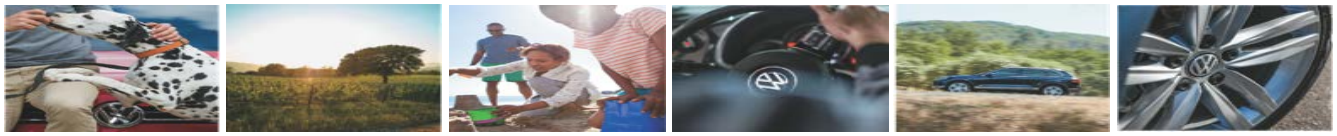
5.19 Private and Virtual Private Networks

Virtual Private Networks (VPN) address privacy and security concerns by providing software that makes the internet appear as a leased connection to the machines being connected.

The most important aspect of a VPN is security. The essential elements of security are 1) access control, 2) authentication, and 3) encryption.

5.19.1 VPN Recommendations

Technology / Resource	Description	Advantage
IPSec	Protocol that implements authentication and encryption	Provides confidentiality, integrity and authentication services
Tunnel Mode (IPSec)	One of two methods used to deploy IPSec	Avoids having to modify PCs, servers and enhances security
3DES (168-bit) or AES	Strong encryption method	Provides strong encryption to ensure privacy
Static IP Addressing	IP address assigned by the ISP which does not change	Simplifies administration, enhances security for location-to-location VPNs
IKE Mode	Internet Key Exchange helps implement IPSec	Enhances security and simplifies administration for VPN clients with dynamic IP addressing from their ISP
Hardware Based Encryption	Encryption processing is done by VPN devices instead of through software by VPN peers	Offers increased performance over software based methods
VPN Devices	Hardware used to create VPNs such as firewalls or VPN concentrators	Using hardware by the same manufacturer to get guaranteed and proven compatibility
Network Suppliers	A vendor who offers network equipment and services	Choosing a reputable network supplier who has knowledge and experience in implementing VPNs will help ensure a reliable and secure network



5.20 Dealership Security

Passwords are an important aspect of dealerships' IT security posture. A poorly chosen password may result in unauthorized access to and/or exploitation of dealership and VWoA's resources. All users, including contractors and vendors with access to systems, are required to take the appropriate measures for securing passwords, as outlined below.

5.20.1 IT Security & Password Recommendations

Item	Minimum	Recommended
Passwords	▪ Expire every 90 days ▪ 8 character minimum using 3 of the following 4: 1) Uppercase, 2) lowercase, 3) numeric and 4) special characters.	▪ Expire every 60 days ▪ 8 character minimum using 3 of the following 4: 1) Uppercase, 2) lowercase, 3) numeric and 4) special characters.
VW Hub e-mail	▪ Maintain VW Hub email as "primary" account ▪ Minimize SPAM to primary account by limiting exclusively to business use.	▪ Minimum requirements, plus maintain VW Hub email on devices that can be wiped clean, if stolen.