

# Automotive Retail Data Security Guidelines – Third Party Providers

---

Most automotive dealers have data processing needs that are not met by the providers of their Dealer Management System (DMS). They select other partners that provide systems or services (Third Party Providers). Third Party Providers include companies providing services or products such as service reminder programs or web sites that display dealer vehicle inventory. Third Party Providers also include companies that provide data extraction or integration services to companies providing services or products. In many cases these Third Party Providers need access to the data stored in the dealer’s DMS. These guidelines address the data security process that these Third Party Providers should undertake to protect the dealer’s data.

The guidelines are color coded into two categories:

Required	The minimum level of data security that should be in place to adequately protect Dealer Data.
Recommended	Additional steps that add further protection of Dealer Data

## 1. Create and maintain an information security policy

**The Information Security Policy is a document created for the internal use of the Third Party Company and any company engaged to certify the compliance of the Company with these Data Security Guidelines. The document should address the appropriate protection of Dealer Data as well as the steps to be taken in the event of a security breach.**

- 1.1. Form a security committee and assign overall responsibility to a senior company executive.
- 1.2. Create a written security policy that:
  - 1.2.1. Addresses all aspects of these guidelines
  - 1.2.2. Addresses each system and network that handles Dealer Data
  - 1.2.3. Identifies all data extracted from or integrated to dealer systems and classifies the data as to its sensitivity or legal status (personal information), and whether the data is stored or merely passed to another party.
  - 1.2.4. Aligns with other industry compliance guidelines as applicable and governmental regulations such as the Gramm-Leach-Bliley Act, Sarbanes Oxley and the Fair Credit Reporting Act
  - 1.2.5. Is updated annually or when the technical or business environment changes affecting security considerations
  - 1.2.6. Is communicated clearly and regularly within the organization
  - 1.2.7. Is communicated externally in an appropriate form
  - 1.2.8. Assigns responsibility for security tasks to specific individuals or teams with appropriate separation of duties
  - 1.2.9. Provides appropriate controls for any outsourced data management or IT that may have access to Dealer Data by:
    - 1.2.9.1. Verifying that any service provider meets these security guidelines
    - 1.2.9.2. Entering into contractual security agreements within any service providers holding them to appropriate security guidelines
  - 1.2.10. Creates a formal process for approving and testing all company controlled external network connections with particular emphasis on connections from the public Internet and those that reach Dealer Data

1.2.11. Encourages a security conscious culture within the organization by integrating security throughout the system lifecycle from requirements definition to testing and maintenance
1.2.12. Documents a data retention and deletion plan
1.2.13. Creates a data backup plan including backup of access controls
1.3. Create and maintain system and network configuration documentation that:
1.3.1. Fully documents all systems and networks including:
1.3.1.1. Network diagrams including wireless networks
1.3.1.2. List of all services and ports necessary for business
1.3.2. Is updated through a formal change control process
1.3.3. Is maintained with strict access controls due to its sensitive nature; a non-sensitive version (e.g. without IP addresses, etc.) may be created for external communication
1.3.4. May be maintained separately from the Information Security Policy and incorporated by reference
1.4. Create incident response plan
1.4.1. Form an incident response team with the responsibility and authority to deal with any security incident
1.4.2. Document an internal escalation procedure to be followed
1.4.3. Establish a process for assessing whether to contact law enforcement in case of breach and for making such contact
1.4.4. Ensure that outsourced data management or IT are obligated to inform the organization of any detected security breaches and the status of any ongoing investigation and progress under a pre-determined timetable
1.4.5. Establish notification procedures for the loss or theft of any mobile devices or data storage devices or media
1.4.6. Link to monitoring and assessment procedures that identify any potential security incidents
1.4.7. Establish post-incident processes to identify potential corrective actions
1.5. Create breach notice process
1.5.1. Designate an individual responsible for managing the breach notice process
1.5.2. Develop a process to determine whether a security breach requires notice
1.5.2.1. Become familiar with applicable state and federal regulations that regulate the need to notify individuals or organizations in the event of a security breach
1.5.2.2. Determine what other circumstances would lead to breach notification
1.5.3. Establish a process for determining who to notify
1.5.4. Establish a process for disseminating the breach notice in a timely fashion
1.5.5. Be prepared to draft a breach notice by considering what information to include, what other resources to provide and other mechanisms to communicate to the effected parties
1.5.6. Be prepared to brief the organization’s employees, management and customer service about a breach and any notice sent

## 2. Create and implement personnel policies that support the security plan

Personnel policies should reinforce the security policy from employee selection and hiring, through training to the safeguarding of data from terminated employees.

- 2.1. Document Employee code of conduct including confidentiality and non-disclosure
- 2.2. Perform background checks to screen new hires who will have access to Dealer Data
- 2.3. Provide new hire and security training with tracking of completion
- 2.4. Provide recurrent security training with tracking of completion
- 2.5. Implement termination procedures relating to physical, system and network access

## 3. Obtain dealer authorization for data integration and data use

Dealers should provide written authorization for the intended uses of Dealer Data as well as acknowledgement of responsibilities of Dealer and Third Party Company.

- 3.1. Obtain written permission from dealer that includes:
  - 3.1.1. General description of the data extraction/integration to be performed
  - 3.1.2. Acknowledgment of responsibilities for each party under various legal guidelines including GLBA, as applicable
  - 3.1.3. Acknowledgment of responsibility for any data integrity issues that ensue from data integration to each system
  - 3.1.4. Authorization to install and execute software on any Dealer system (including the Dealer Management System) unless the system is provided by the Third Party Provider
- 3.2. Provide, upon Dealer request, details of data extraction or integration including:
  - 3.2.1. Specific list of data items extracted or updated from each system
  - 3.2.2. Frequency of data extractions or expected frequency and duration of connectivity for integration
- 3.3. If required, obtain user-id and password from dealer
  - 3.3.1. User-id should be assigned for the exclusive use of the organization
  - 3.3.2. Third Party Provider should request that Dealer only grant access to required data

## 4. Protect Dealer Data within Third Party controlled environment<sup>1</sup>

Third Party Company should provide protection of Dealer Data in its control from the transmission of the data through the storage of the data in any form.

<sup>1</sup> Refer to STAR Dealer Infrastructure Guidelines for recommendations for securing dealership data environment.

4.1. Build and maintain a secure network, systems and applications environment
4.1.1. Configure all systems to provide appropriate security
4.1.1.1. Disable unused ports
4.1.1.2. Disable any unnecessary and insecure services and protocols
4.1.1.3. Enable system locks to prevent access after inactivity period
4.1.2. Install and configure anti-malware software for all devices or systems subject to infection
4.1.2.1. Ensure that automatic downloads and updates are utilized
4.1.2.2. Perform regular scans for viruses and other malware on all devices or systems subject to infection
4.1.3. Install security patches on a timely basis
4.1.4. Maintain secure websites
4.1.4.1. Ensure that any web pages that allow users to transmit sensitive information use HTTPS or another equivalent security method
4.1.4.2. Mask account and credit card numbers
4.2. Protect stored data
4.2.1. Do not store Dealer Data for longer than is reasonably necessary to provide Third Party's product or service or as mandated by governmental requirements
4.2.2. Control access to Dealer Data that is stored by the organization
4.2.2.1. No device should be accessible through the vendor supplied default user ID or password
4.2.2.2. Assign individual users unique user IDs
4.2.2.3. Assign appropriate authentication methods
4.2.2.3.1. Use passwords or other secure authentication methods for access to systems and non-sensitive information
4.2.2.3.2. Use two-factor identification for access to sensitive information
4.2.2.3.3. Implement a secure password usage policy
4.2.2.4. Assign system and network access privileges based on job responsibility
4.2.2.5. Use session timeouts to force logouts after inactivity period
4.2.2.6. Delete accounts for inactive users, and terminated employees and contractors
4.2.3. Provide additional protection for storage of sensitive information
4.2.3.1. Provide additional access control for the access or download of any sensitive information
4.2.3.2. Encrypt stored sensitive information and protect encryption keys
4.2.3.3. Utilize additional firewall layers to protect sensitive information
4.2.4. Install and maintain a firewall configuration
4.2.4.1. Implement a firewall at each Internet connection
4.2.4.2. Establish a firewall between any DMZ and Intranet connection
4.2.5. Restrict and control physical access to data center
4.2.5.1. Ensure that data center is physically secure including:
4.2.5.1.1. Secure entrance using physical security measures such as biometrics, keys or passes
4.2.5.1.2. Equipment housing sensitive data should be adequately protected with locked racks or cages
4.2.5.2. Restrict data center access to those with business needs
4.2.5.3. Control and track physical access devices such as keys or passes
4.2.5.4. Track data center access

4.2.5.5. Monitor all data center storage devices for removal from the network or systems
4.2.5.6. Maintain logging for any removable storage devices or media used in the data center
4.2.5.7. Secure any printouts or media containing sensitive information
4.3. Protect transmission of data
4.3.1. Use a secure network method to transmit Dealer Data
4.3.2. Encrypt the transmission of any sensitive information sent over the public Internet
4.3.3. Promote and support the encryption of sensitive information sent over the public Internet
4.3.4. Use wireless encryption to transmit any sensitive information to or from wireless devices
4.3.5. Insure that any Dealer Data transmitted outside the company is delivered to a secure location

## 5. Actively monitor, review and revise policies, access and systems

Given the changing nature of systems, security threats and Dealer requirements the information security plan and implementation should be monitored and revised as appropriate.

5.1. Assess and prioritize security risks in:
5.1.1. Employee hiring training and management
5.1.2. Systems and networks
5.1.3. Physical data storage
5.2. Conduct regular security audits to include:
5.2.1. Review of all internal and external systems and network
5.2.2. Validation of firewall configurations using vulnerability tools
5.2.3. Application level assessments to ensure application and database security
5.2.4. Audits of any outsourced data management or IT
5.2.5. Review of unusual Internet activity, email and network traffic
5.2.6. Mock situation reviews to test the ability to respond to security threats
5.2.7. Check for unauthorized external access capability
5.3. Monitor public information about security threats and vulnerabilities
5.4. Monitor all access
5.4.1. Implement and monitor intrusion detection tools
5.4.2. Review physical access logs
5.4.3. Implement and review automated audit trails for all system components
5.5. Implement procedures for employees to report any suspicious activity whether initiated internally or externally
5.6. Test security systems and processes
5.7. Test backup procedures

<b>6. Definitions</b>	
6.1. Sensitive information	
6.1.1.	Data that is identifiable to an individual and has the potential to harm or embarrass the subject
6.1.2.	Examples include: Social Security Number Driver's License Number Address information Emergency contact information Birth dates Credit Card numbers Account numbers Passwords or PINs Criminal arrests or convictions Judgments in civil cases Medical information Race, ethnicity, national origin Data concerning sexual orientation or activity Financial data Credit scores, tiers and decisions Salary and compensation Disability status
6.2. Dealer Data	
6.2.1.	Data owned by a dealer and stored in a dealer licensed application
6.3. Employee	
6.3.1.	Personnel engaged on a full-time, part-time or contract basis by the Third Party
6.4. Third Party Provider	
6.4.1.	Company that provides services or products to automotive dealers that make use of Dealer Data (e.g. service reminder programs or web sites that display dealer vehicle inventory)
6.4.2.	Company that provides data extraction or integration services to companies providing such services or products.