

# INFORMATION SECURITY PROGRAM

Dealership Name: \_\_\_\_\_

Program Coordinator: \_\_\_\_\_  
(Name and/or Employment Title)

## Program Overview

### Objectives:

- Insure the security and confidentiality of the Dealership's (our) customer information.
- Protect against loss or destruction of our customer information.
- Protect against unauthorized access to or use of customer information

“Customer information” means personally identifiable financial information that we obtain about our customers. It includes information a consumer provides us in order to obtain credit, a lease or insurance. It also includes information about customers that we receive from financial institutions and credit reporting agencies.

Our Program Coordinator has primary responsibility for overseeing the implementation and maintenance of this program. The Program Coordinator is an employee of our dealership.

## Risk Assessment

The Program Coordinator has assessed our Dealership to identify unresolved risks to the security, confidentiality and integrity of customer information in the following areas:

- Hiring, managing and training our employees;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- Detecting, preventing and responding to attacks, intrusions or other systems failures.

What follows are safeguards designed to address the risks in each category:

### Hiring, Managing and Training Our Employees

Dealership implements the following employee management and training safeguards:

1. All Dealership employees are responsible for complying with the Information Security Program.
2. The Dealership will make reasonable inquiry and check references of each potential employee prior to the commencement of the applicant's employment.
3. All current and new employees who have access to customer information will participate in the Dealership's information security training. This training will include basic steps to maintain the security, confidentiality and integrity of customer information.
4. Dealership employees will not be permitted to use or reproduce customer information for their own use or for any use not authorized by the Dealership.
5. All employees who fail to comply with the Dealership's Program will be subject to disciplinary measures, up to and including termination of employment.

## **Information Systems - Information Security Policies and Procedures**

Dealership implements the following information systems safeguards:

1. Paper-based customer information will not be left exposed and unattended in an unsecured area.
2. Electronic transmissions of customer information will be performed to the greatest degree reasonable on a secure basis.
3. Records containing customer information will be stored and secured as follows:
  - Paper records will be stored in a room or file cabinets that are locked or otherwise not available to the general public.
  - Electronic customer information will be stored on secure servers. Access to such information will be password controlled, and the Program Coordinator will control access to such servers.
  - All electronic customer information will be backed up on a regular basis.
4. All customer information will be disposed of in a secure manner.
  - Paper based customer information will be shredded prior to disposal.
  - Electronic information will be effectively deleted prior to hardware disposal.

## **Intrusions or Other Systems Failures**

In keeping with the objectives of the Program, the Dealership will implement, maintain and enforce the following attack and intrusion safeguards:

1. The Program Coordinator will maintain adequate procedures to address any breaches of the Dealership's information safeguards.
2. The Program Coordinator will maintain a working knowledge of widely available technology for the protection of customer information.
3. The Dealership will utilize anti-virus software.
4. The Dealership will maintain computer firewalls.

## **Audit**

The Program Coordinator will monitor the effectiveness of the Dealership's safeguards' key controls, systems, and procedures, to ensure that all safeguards implemented as a result of the risk assessment are effective to control the risks identified in the risk assessment. The Program Coordinator will revise current safeguards and/or implement new safeguards as necessary to ensure the continued viability of the Program.

## **Overseeing Service Providers**

The Program Coordinator will be responsible for overseeing the Dealership's service providers who handle or have access to customer information. The Program Coordinator will take reasonable steps to select and retain service providers that are capable of maintaining safeguards to protect the specific customer information handled or accessed by each service provider that are consistent with the level of safeguards employed by the Dealership for such information.

## **Periodic Reevaluation of the Program**

The Program Coordinator will reevaluate and modify the Program from time to time as appropriate.