EARNHARDT INFORMATION SECURITY PROGRAM

PROGRAM OBJECTIVES

The objectives of this Information Security Program ("Program") are as follows:

- Insure the security and confidentiality of all Earnhardt Dealership's ("Dealership") customer information.
- Protect against any anticipated threats or hazards to the security and/or integrity of the Dealership's customer information.
- Protect against unauthorized access to or use of the Dealership's customer information that could result in substantial harm or inconvenience to any customer.

For purposes of the Program, "customer information" means any information about a customer of the Dealership, or information the Dealership receives about the customer of another financial institution, which can be directly or indirectly attributed to the customer. This Program, in and of itself, does not create a contract between the Dealership and any person or entity.

PROGRAM COORDINATOR(S)

This Program and the safeguards it contemplates shall be implemented and maintained by the **Corporate Program Coordinator** ("CPC") and individual **Dealership Program Coordinators** ("DPCs").

DPCs will be selected for the following location programs:

1. Earnhardt Ford
2. Earnhardt Gilbert Dodge (CJDR)
3. Earnhardt Honda (Honda)
4. Rodeo Ford
5. San Tan Hyundai
6. Earnhardt Enterprises (Toyota)
7. Earnhardt Buick GMC
8. Earnhardt Avondale Hyundai
9. Human Resources (HR)
10. Information Technology (IT)
11. Marketing
12. Business Dev. Center (BDC), as applicable
13. Mr. Ed
14. Vendors / Service Providers
15. Earnhardt Kia
16. Earnhardt Hyundai North Scottsdale
15. Earnhardt Savings Plan
16. Earnhardt Comprehensive Health and Welfare Benefit Plan
17. Earnhardt Cadillac
18. Earnhardt Chandler Cadillac
19. Earnhardt Lexus
20. Rodeo Kia
21. Peoria Kia
22. Earnhardt Liberty Kia
23. Earnhardt Mazda
24. Earnhardt Maserati
25. San Tan VW
26. Earnhardt Buick GMC Las Vegas
27. Earnhardt Mazda Las Vegas
28. Rodeo Hyundai
29. Earnhardt Chevrolet

The CPC shall design, implement and maintain new safeguards as are determined to be necessary from time to time. The DPCs shall report to the CPC. The CPC may delegate or outsource the performance of any function under the Information Security Program as deemed necessary from time to time.

In the event the CPC leaves the employment of the Dealership, Earnhardt General Counsel shall take over the responsibilities of the CPC until a new CPC is designated. In the event a DPC leaves the employment of the Dealership, the CPC will appoint a new DPC.

RISK ASSESSMENT

All DPCs shall conduct a risk assessment of their location to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in its unauthorized disclosure, misuse, alteration, destruction or other compromise, and assess the sufficiency of any safeguards in place to control these risks.

The risk assessment shall cover all relevant areas of the Dealership's operations, as determined by the CPC. At a minimum, the risk assessment shall cover the following:

- Employee training and management;
- 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.

Once the DPC has identified the reasonably foreseeable risks to the Dealership's customer information, the DPC and CPC will determine whether the Dealership's current policies and procedures in these areas sufficiently mitigate the potential risks identified. If not, the CPC shall design new policies and procedures that meet the objectives of the Program.

AUDIT

The CPC shall periodically test or audit the effectiveness of the Dealership's safeguards, primary 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 CPC shall revise current safeguards and/or implement new safeguards as necessary to ensure the continued viability of the Program.

OVERSEEING SERVICE PROVIDERS

The Information Technology and Vendor/Service Providers DPCs shall be responsible for overseeing the Dealership's service providers who handle or have access to customer information and shall 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.

Service provider contracts shall be reviewed prior to their execution by the Dealership to ensure that each contract contains appropriate obligations of the service provider to comply with safeguarding requirements.

PERIODIC REEVALUATION OF THE PROGRAM

The CPC shall reevaluate and modify the Program from time to time as the CPC deems appropriate. The CPC shall base such reevaluation and modification on the following:

- The results of the CPC's monitoring efforts;
- Any material changes to the Dealership's operations, business or information technology arrangements; or
- Any other circumstances that the CPC knows, or has reason to know, may have a material impact on the Program.

In order to assist the CPC in this regard, the DPCs and Dealership management shall keep the CPC apprised of the nature and extent of all third party relationships and any operational changes or other matters that may impact the security or integrity of the Dealership's customer information.

INFORMATION SECURITY POLICIES AND PROCEDURES

Employee Training and Management:
In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following employee management and training safeguards:

1. All employees and independent contractors are responsible for complying with the Dealership's Program.
2. All employees shall sign the "Employee Acknowledgement of and Agreement to Comply with the Earnhardt Information Security Program."
3. The Dealership will check references of each potential employee prior to the commencement of the applicant's employment.
4. The Dealership will obtain a consumer report and criminal background check of each applicant prior to the commencement of the applicant's employment.
5. All offers of employment shall be subject to satisfactory references and consumer/criminal report investigations.
6. All new employees, and independent contractors who perform services in the Dealership, who have access to customer information will participate in the Dealership's information security training. Each person shall sign and acknowledge his or her agreement to abide by the Dealership's Program. Training will recur periodically as determined by the CPC and as required by changes to the Program.
7. Such training program shall include, at a minimum, basic steps to maintain the security, confidentiality and integrity of customer information and shall include the following:

    - For All Locations:
        - The types of customer information subject to protection under the Information Security Program will be identified for employees and independent contractors.
        - Each employee will sign an agreement acknowledging the policy and agreeing to abide by its terms.
        - Rooms and file cabinets where paper records are kept will be kept locked when unattended to the extent possible.
        - Password-activated computer software will be used to the extent possible.
        - Systems, applications and terminals will utilize an automatic log-off function that terminates access after a period of inactivity.
        - Strong passwords (at least eight characters long and alphanumeric) will be used.
        - Passwords will be changed periodically, and the security of passwords will be maintained.
        - To the extent possible, electronic information will be sent only over secure channels.
        - Paper and electronic records will be disposed of properly. Shredders will be available for this purpose.
        - **Sharing of passwords is expressly prohibited.**
    - In addition, for locations with a Business Office, for the Human Resources Department and for the Legal/Administrative Department:
        - Deal Jackets shall be stored in a room, cabinet, or other container that is locked when unattended.

- All storage areas shall be reasonably protected against destruction or potential damage from physical hazards.
- Log-out and log-in records will be maintained for tracking of all deal jackets that leave the business office.

- For the Business Development Center (BDC), as applicable:
  - Each employee will have an individual log-in and will log-out of computer when away from work station.
  - Any requests by customers for sensitive information will be referred to the manager of the BDC. The customer will be required to provide identification to obtain information.
  - Computer generated printouts will be locked in a file cabinet and destroyed after information is used.

8. The Dealership will take appropriate steps to encourage awareness of and compliance with the Program.
9. All employees and independent contractors will be permitted to access customer information only on a "need-to-know" basis as determined by Dealership management.
10. Personnel shall not be permitted to access, use or reproduce customer information, whether electronic or non-electronic, for their own use or for any use not authorized by the Dealership.
11. All persons who fail to comply with the Dealership's Program shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for independent contractors that perform services in the Dealership.
12. The Dealership will promptly notify the IT department of any employee that is terminated or otherwise ceases working for Earnhardt's so that their log-in and password may be immediately removed from the system.
13. Customer information will be provided to outside third parties in response to subpoena or other legal process, upon written request of the customer, if the outside third party is a party to whom disclosure of the information previously was authorized, or in such situations as shall be identified from time to time by the CPC and as are consistent with state and federal protection of customer information.

Information Systems

In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following information systems safeguards:

1. All records containing customer information shall be stored and maintained in a secure area.
   - For all locations:
     - To the extent possible, electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the IT Department shall control access to such servers.
     - To the extent possible, customer information consisting of financial or other similar information (e.g., social security numbers, etc.) shall not be stored on any computer system with a direct Internet connection.
     - Servers storing customer information consisting of financial or other similar information (social security numbers, etc.) will not be readily accessible via outside dial up. All parties requesting access to the server will be required to be on the "Approved 3rd Party Vendor" list and must contact the IT department prior to accessing the data.
     - To the extent possible, all customer information will be backed up on a daily basis. Such back up data shall be stored in one or more fire-resistant secure locations.

- Server locations are secured with access restricted to the IT Department, and access can be electronically audited.

2. All electronic transmissions of customer information, whether inbound or outbound, shall be performed on a secure basis to the extent possible.
   - For all locations:
     - Inbound credit card information, credit applications, or other sensitive financial data transmitted to the Dealership directly from consumers shall use a secure connection, such as a Secure Sockets Layer (SSL) or other currently accepted standard, so that the security of such information is protected in transit. Such secure transmission shall be automatic. Consumers shall be advised against transmitting sensitive data, like account numbers, via electronic mail.
     - Inbound transmissions of customer information delivered to the Dealership via other sources be encrypted or otherwise secured.
     - Outbound transmissions of customer information shall be secured in a manner acceptable to the CPC.
     - To the extent sensitive data must be transmitted to the Dealership by electronic mail, such transmissions shall be password controlled or otherwise protected from theft or unauthorized access at the discretion of the CPC.
     - The IT Department shall review all vendor applications to ensure an appropriate level of security both within the Dealership and with the Dealership's business partners and vendors.
   - For locations with a Sales and/or Finance Department:
     - Fax machines will be preprogrammed with the fax numbers of lending institutions with which the Dealership regularly does business.

3. All paper transmissions of customer information by the Dealership shall be performed on a secure basis.
   - For all locations:
     - Sensitive customer information shall be properly secured at all times.
     - Customer information delivered by the Dealership to internal recipients or third parties shall be kept sealed in an interoffice envelope or the equivalent at all times.

4. All customer information shall be disposed of in a secure manner.
   - For all locations:
     - The CPC shall audit the disposal of all records containing customer information.
     - Paper based customer information shall be shredded and stored in a secure area until a disposal or recycling service picks it up.
     - All hard drives, diskettes, magnetic tapes, or any other electronic media containing customer information shall be erased and/or destroyed prior to disposing of computers or other hardware.
     - All hardware shall be effectively destroyed.
     - All customer information shall be disposed of in a secure manner after any applicable retention period.

5. The IT Department shall maintain an inventory of Dealership computers, including any handheld devices or PDAs owned by the Dealerships, on or through which customer information may be stored, accessed or transmitted. Employees who use personal handheld devices for Dealership purposes are required to sign an agreement controlling the security of the device and use of information.

6. The CPC shall develop and maintain appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information.

Detecting, Preventing and Responding to Attacks, Intrusions or Other Systems Failures
In keeping with the objectives of the Program, the Dealership shall implement, maintain and enforce the following attack and intrusion safeguards:

1. The IT Department and CPC shall ensure the Dealership has adequate procedures to address any breaches of the Dealership's information safeguards that would materially impact the confidentiality and security of customer information. The procedures shall address the appropriate response to specific types of breaches, including hackers, general security compromises, denial of access to databases and computer systems, etc.
2. The IT Department shall utilize and maintain a working knowledge of widely available technology for the protection of customer information.
3. The CPC shall communicate with the IT Department from time to time to ensure that the Dealership has installed the most recent patches that resolve software vulnerabilities.
4. The Dealership shall utilize anti-virus software that updates automatically.
5. The Dealership shall maintain up-to-date firewalls.
6. The IT Department shall manage the Dealership's information security tools for employees and pass along updates about any security risks or breaches.
7. The IT Department shall establish procedures to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure.
8. The IT Department shall ensure that access to customer information is granted only to legitimate and valid users.
9. The IT Department shall notify the Legal Department promptly if customer information is subject to loss, damage or unauthorized access. The IT Department shall also notify the CPC of such situations.