Information Security Policies and Procedures – Information Systems

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

(Safeguards may include the following, as applicable to your Dealership. Note that this is by no means a complete list, nor are the safeguards it contains necessarily appropriate for your Dealership. Ensure your use of any of the following safeguards is consistent with state and local law):

1. All records containing customer information shall be stored and maintained in a secure area
   - Paper records shall be stored in a room cabinet, or other container that is locked when unattended access to such areas shall be controlled.
   - All target areas shall be protected against destruction or potential damage from physical hazards like fire or floods.
   - Electronic customer information shall be stored on secure servers Access to such information shall be password controlled and access to such servers shall be controlled.
   - 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.
   - All customer information shall be backed up on a daily basis. Such back up data shall be stored in a secure location.

2. All electronic transmissions of customer information, whether inbound or outbound, shall be performed on a secure basis.
   Inbound credit card information, credit applications, or other sensitive financial data transmitted to the Dealership directly from the 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.
   - The Dealership shall require by contract that inbound transmissions of customer information delivered to the Dealership via other sources be encrypted or otherwise secured.
   - All outbound transmissions of customer information shall be secured. To the extent that if 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.
   - Vendors will routinely be audited to ensure appropriate levels of security and compliance to safeguarding customer information.

3. All paper transmissions of customer information by the Dealership shall be performed on a secure basis.
   - Sensitive customer information shall be properly secured at all times.
   - Customer information delivered by the Dealership to third parties shall be kept sealed at all times.
   - Paper-based customer information shall not be left unattended at any time it is in an unsecured area.

4. All customer information shall be disposed of in a secure manner.
    - Proper disposal of information will be monitored and corrective action implemented if found not in compliance.
    - 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. All equipment will routinely be inventoried to ensure customer information is not stolen or lost. Personal or unauthorized equipment will not be allowed. Unauthorized equipment will be removed.

6. Burt Watson Chevrolet, Inc. shall develop and maintain appropriate oversight or audit procedures including monitoring to detect the improper disclosure or theft of customer information.

Information Security Policies and Procedures-Detecting, Preventing and Responding to Attacks, Intrusions or Other System Failures

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

I. 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 data bases and computer systems, etc.

II. Utilize and maintain a working knowledge of widely available technology for the protection of customer information.

III. The systems administrator shall communicate with the Dealership's computer vendors from time to time to ensure that the Dealership has installed the most recent patches that resolve software vulnerabilities.

IV. The Dealership shall utilize anti-virus software that updates automatically.

V. The Dealership shall maintain up-to-date firewalls.

VI. The systems administrator shall manage the Dealership's information security tools for employees and pass along updates about any security risks or breaches.

VII. The systems administrator shall establish procedures to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure.

VIII. The systems administrator shall ensure that access to customer information is granted only to legitimate and valid users.

IX. The Program Coordinator or designee shall notify customers promptly if their customer information is subject to loss, damage or unauthorized access.