PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS

Our Program Coordinator

We have appointed Robert P. Grow, Jr. as the Program Coordinator of our Dealership's Information Security Program. The Program Coordinator will report directly to Clete Landis the Owner / president of the Dealership. In the event the Program Coordinator ceases to be employed by the Dealership or is unable to perform his/her responsibilities, Keith Muir shall take over the responsibilities of the Program Coordinator until a new permanent Program Coordinator is appointed.

The Program Coordinator's Responsibilities

It is the Program Coordinator's responsibility to design, implement and maintain privacy policies and information safeguard standards as he/he determines to be necessary from time to time. Specific responsibilities that have been delegated to the Program Coordinator include:

Identifying and assessing the risks to customer information in each relevant area of the Dealership's operation, and evaluating the effectiveness of current safeguards that have been implemented to control these risks.

Designing and implementing privacy policies and information security standards that are appropriate for the size and complexity of our Dealership and its operations, the nature and scope of our activities and the sensitivity of the customer information we collect, store and share with others.

Regularly monitoring and testing the privacy policies and information security standards.

Assisting with the selection of appropriate service providers that can maintain safeguards to protect the relevant customer information and reviewing service provider contracts to ensure that each contracts contain appropriate obligations with respect to the use of customer information and the implementation of safeguards.

Evaluating and adjusting the Dealership's Privacy Policies and Information Security Standards in light of relevant circumstances, including changes to the Dealership's operations, business relationships, technological developments and/or other matters that may impact the security or integrity of the Dealership's customer information.

Pursuant to the USA Patriot Act and the Rules adopted by the Financial Crimes Enforcement Network (FinCEN), a Bureau under the Department of Treasury, the Program Coordinator will also be the contact person for Law Enforcement Agencies to communicate the names of suspected terrorists and money launders in an effort to locate and secure accounts and transactions involving those suspects. Upon receiving a request for information from FinCEN, the Program Coordinator will:

Provide FinCEN with his/her name, title, and appropriate contact information, such as a mailing address, email address, telephone number and facsimile number, and notify FinCEN promptly of any modifications with respect to contact information.

Ensure that current accounts maintained by the Dealership, any accounts maintained by the Dealership during the past 12 months, and any transactions conducted during the past 6 months that the Dealership is required by law or regulation to record or that the Dealership has recorded and maintained are searched for the names provided by FinCEN.

If the Dealership has entered into a transaction with an individual or entity on the list, send a Report to FinCEN that contains: (1) The name of the individual, entity or organization; (2) The account numbers or, in the case of transactions, the date and type of each transaction; and (3) The social security number, taxpayer identification number, passport number, date of birth, address, or other personal identifying information provided by the individual or entity at the time of the transaction.

Questions about the scope or terms of a request will be directed to the Law Enforcement Agency that sent the request for information to FinCEN, but the Report will be sent to FinCEN, not the Law Enforcement Agency that requested the search, unless the Program Coordinator is instructed otherwise.

Employee Management and Training

All current employees and new hires, as well as independent contractors who perform services on behalf of the Dealership, will:
Be subject to satisfactory reference and consumer/criminal report investigations, where appropriate.
Only have access to customer information if they have a business reason for seeing it.
Participate in the Dealership's privacy policies and information security standards training program and attend educational and training seminars on a regular basis.
Sign and acknowledge his/her agreement to our Dealership's Statement of Privacy Policies and Information Security Standards.
Be responsible for protecting the confidentiality and security of the customer information our Dealership collects and for using the information in accordance with our Privacy Policies.
Not be permitted to post passwords near their computers or share passwords with any other person.
Refer telephone calls or other requests for customer information to the Program Coordinator or appropriate manager when such requests are not received within the ordinary course of the Dealership's business or are for information that the employee is not authorized to provide.
Disclose to service providers, marketers or any other parties only that customer information which is necessary to complete a transaction initiated by the customer and/or as permitted by law. If an employee is unsure as to whether a specific disclosure is permitted, he or she will be instructed to check with the Program Coordinator or appropriate manager to verify that it is acceptable to release the information before doing so.
Be required to notify the Program Coordinator or appropriate manager immediately of any attempts by unauthorized persons to obtain access to customer information and/or if any password or customer information is subject to unauthorized access.
Any employee that fails to abide by our Statement of Privacy Policies and Information Security Standards, whether such failure is intentional or unintentional, will be subject to appropriate disciplinary action, which may include termination of employment.
When an employee ceases to be employed by the Dealership, he/she will be required to turn in any keys in his/her possession that provide access to the Dealership and file cabinets, desks, and offices in the Dealership; passwords and security codes, if applicable, will be deleted; and employees will not be permitted to take any customer information from the Dealership.

Obtaining Customer Information and Verifying Customer Identities
The following procedures will be implemented with respect to obtaining customer information and verifying customer identities:
Forms utilized by the Dealership request customer information, such as names, addresses, telephone numbers, birth dates, social security numbers, tax identification numbers, and driver's license and insurance
information, to enable the Dealership to verify the identification of its customers. In addition, customers must sign documentation, including sworn statements in some cases, wherein the customer represents and warrants that he/she is the person identified in the documentation.
Employees will request to see the customer's driver's license or other form of government-issued identification bearing a photograph to verify the customer's identity and will make a copy of the same to retain in the customer's file. If a customer requests financing in connection with a transaction, the customer will be required to provide employment information and references and must authorize the Dealership to obtain a credit report, all of which may be utilized to verify the identity of the customer. Employees may also request copies of the customer's utility bills, bank or credit card statements and paycheck stubs.
In the event that customer information provided in documentation is conflicting or cannot be verified upon further inquiry, employees shall request additional government-issued documentation evidencing the customer's residence and bearing a photograph or other safeguard (i.e. a social security card, alien

identification card, or passport) to enable employees to form a reasonable belief that they know a customer's identity. When appropriate, employees shall write a summary of the means and results of any measures taken to identify a customer, including the resolution of any discrepancy in the identifying information obtained. Employees will be instructed to notify the Program Coordinator if customer information still cannot be verified.
The Dealership has access to updated versions of the alphabetical master list of Specially Designated Nationals and Blocked Persons maintained by the Office of Foreign Asset Control (OFAC), which will be checked to ensure that potential customers do not appear on the same.
Paper and electronic records containing customer information and relevant to the Dealership's identity verification process will be retained by the Dealership in accordance with federal and state record retention requirements. Upon the expiration of the appropriate retention period, any such records will be disposed of in a secure manner in accordance with the Dealership's information security standards.

Information Systems
The following information security standards will be implemented in order to protect customer information collected and maintained by our Dealership:
Employees will have access only to that customer information which is necessary to complete the designated responsibilities. Employees shall not access or provide any other unauthorized person access to customer information that is obtained during the course of employment. Requests for customer information that are outside the scope of the Dealership's ordinary business or the scope of an employee's authorization must be directed to the Program Coordinator or designated individuals.
Access to electronic customer information will be password controlled. Every employee with access to the Dealership's computer system and electronic records will have a unique password consisting of at least 6 characters, including numbers and letters. Only employees that need to access electronic records will be provided with passwords.
All paper and electronic records will be stored in secure locations to which only authorized employees will have access. Any paper records containing customer information must be stored in a deal jacket or folder.
Paper records must be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records will be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records will be maintained in a fireproof file cabinet and/or at an offsite location. Customers, vendors and service providers shall not be left in an area with insecure customer records.
Backups of the computers and/or server will be made at least once each day, or at more frequent intervals as deemed necessary. At least once each month the backup information will be verified. Backup disks will be stored in a locked file cabinet.
Virus protection software has been installed on the computers and new virus updates will be checked at regular intervals. All computer files will be scanned at least once each month, or at more frequent intervals as deemed necessary.
Firewalls and security patches from software vendors will be downloaded on a regular basis.
All data will be erased from computers, disks, hard drives or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives will be removed and destroyed. Any paper records will be shredded and stored in a secure area until an authorized disposal/recycling service picks it up.
Employees will be instructed to log off all Internet, E-mail and other accounts when they are not being used. Employees will not be permitted to download any software or applications to Dealership computers or open e-mail attachments from unknown sources. Electronic records may not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator.
Electronic records will not be stored online and are not accessible from the Internet. If customer information is transmitted electronically over external networks, employees will be instructed to encrypt the information at the time of transmittal.

Neither current nor former employees will be permitted to remove any customer information from the Dealership, whether contained in paper records or electronic records, or to disclose our information security standards to any person without authorization from the Program Coordinator.

Selection and Oversight of Service Providers

In order to protect the customer information our Dealership collects; we will take steps to evaluate and oversee our service providers. The following evaluation criteria will be utilized in selecting service providers:

Compatibility and willingness to comply with the Dealership's privacy policies and information security standards and the adequacy of the service provider's own privacy policies and information security standards.

Records to be maintained by the service provider and whether the Dealership will have access to information maintained by the service provider.

The service provider's knowledge of regulations that are relevant to the services being provided, including privacy and other consumer protection regulations.

Experience and ability to provide the necessary services and supporting technology for current and anticipated needs.

Functionality of any service or system proposed and policies concerning maintaining secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions.

Service and support that will be provided in terms of maintenance, security, and other service levels.

Financial stability of the service provider and reputation with industry groups, trade associations and other dealerships.

Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer service; rights to modify existing services performed under the contract; warranty, confidentiality, indemnification, limitation of liability and exit clauses; guidelines for adding new or different services and for contract re-negotiation; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; insurance coverage to be maintained by the service provider; and use of the Dealership's data, equipment, and system and application software.

The right of the Dealership to audit the service provider's records, to obtain documentation regarding the resolution of disclosed deficiencies, and to inspect the service provider's facilities.

Service Providers will be required to agree contractually to be responsible for securing and maintaining the confidentiality of customer information, including agreement to refrain from using or disclosing the Dealership's information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use or disclosure of customer and Dealership information, to comply with applicable privacy regulations, and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect the Dealership or its customers and to notify the Dealership of the services provider's corrective action.

Service providers will be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance.

Managing System Failures

The Program Coordinator will implement audit and oversight procedures as he/she deems necessary to detect the improper disclosure or theft of customer information and to ensure that employees, independent contractors and service providers are complying with our Dealership's Privacy Policies and Information Security Standards.

If the Dealership's Privacy Policies and Information Security Standards are breached, the Program Coordinator will inform Clete Landis, the Owner / President of the Dealership.

The Program Coordinator and Clete Landis will take appropriate steps to notify counsel, service

providers and customers of any breach, damage or loss of information and the risks associated with the same and will immediately take measures to limit the effect of the breach, identify the reason for the breach and implement procedures to prevent further breaches.
In the event of a breach, or at any other time as the Program Coordinator deems appropriate, the Program Coordinator may modify or supplement our Dealership's Privacy Policies and Information Security Standards.

EMPLOYEE AGREEMENT TO COMPLY WITH PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS

Effective July 1, 2001, the Financial Services Modernization Act of 1999, more commonly known as the "Gramm-Leach-Bliley Act", requires "financial institutions" that collect nonpublic personal information about customers who obtain a "financial product or service" to: (1) Implement privacy policies and procedures to protect the information they collect; and (2) Provide their customers with certain notices, including an Initial Privacy Policy Notice and, if applicable, an Annual Notice. In addition, as of May 23, 2003, any financial institution that collects personal information from their customers must comply with the Federal Trade Commission's Safeguards Rule, which requires financial institutions to develop a written information security plan that describes their program to protect customer information. In certain circumstances, our Dealership is deemed to be a "financial institution" for purposes of the Gramm-Leach-Bliley Act and the Federal Trade Commission's Implementing Rules. As a condition of your employment with our Dealership, you agree to:
1. Read the "Statement of Privacy Policies and Information Security Standards" and familiarize yourself with the information contained therein.
2. Follow our procedures for providing a copy of our Privacy Policy to each customer.
3. Follow our procedures for safeguarding and protecting customer information in accordance with our "Statement of Privacy Policies and Information Security Standards".

BY SIGNING BELOW, I ACKNOWLEDGE THAT I HAVE RECEIVED AND READ THE STATEMENT OF PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS AND AGREE TO COMPLY WITH THE PRIVACY POLICIES AND INFORMATION SECURITY STANDARDS AS SET FORTH THEREIN AS A CONDITION OF MY EMPLOYMENT. I FURTHER UNDERSTAND THAT THE FAILURE TO FOLLOW THE DEALERSHIP'S PRIVACY POLICIES AND INFROMATION SECURITY STANDARDS MAY RESULT IN DISCIPLINARY ACTION, INCLUDING THE TERMINATION OF MY EMPLOYMENT.

_____ _____

EMPLOYEE DATE

_____ _____

WITNESS DATE