Information Security Program
Brakke Implement, Inc.

Program Scope

This program is designed to implement physical, administrative, and technical safeguards of the Personal Data we collect from our customers. "Personal Data" includes an individual customer's last name and first name or first initial, a customer's social security or other identification number, financial or transactional information, any private access code or PIN, contact or address information, or any other personally identifying information. Personal Data also includes any additional information required by applicable law to be protected but does not include any publicly available information.

Program Coordinator

LeAnn Doyle is designated as the Program Coordinator of our Dealership's Information Security Program until such Coordinator is replaced by the Dealership. The Program Coordinator reports directly to General Manager of the Dealership. In the event the Program Coordinator ceases to be employed by the Dealership or is unable to perform his/her responsibilities then a new Program Coordinator will be appointed, and in the interim period, General Manager shall serve as the interim Program Coordinator.

It is the Program Coordinator's responsibility to design, implement and maintain the Dealership's privacy policies and information security program as he/she determines to be necessary from time to time based upon the size of the business and scope of the business activities. The Program Coordinator's specific responsibilities include:

- Identifying and assessing the risks to Personal Data in each relevant area of the Dealership's operation, and evaluating the effectiveness of current safeguards that have been implemented to control these risks. These risks include but are not limited to:
    - Intentional or unintentional breaches of Personal Data by our employees or agents.
    - Hacking, spoofing, phishing, malware, or other malicious programs, schemes, or devices to gain access to Personal Data by unauthorized individuals.
    - Failure of a third party vendor to properly secure and encrypt the transmission or storage of Personal Data.
    - Inadvertent disclosure of a customer's Personal Data to another customer.
    - Natural disasters or similar events disrupting our security measures.
- Designing and implementing privacy policies, information security programs, and identity theft prevention programs 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 Personal Data we collect, store and share with others and any other data security related programs or policies required by law.
- Evaluating and adjusting the Dealership's privacy policies, information security programs, and identity theft prevention programs 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 Personal Data.

- Coordinating the Dealership's response to any breach of the Dealership's privacy policies, information security programs, identity theft prevention programs or other policies or applicable laws.
- Assisting with the selection of appropriate service providers.

Employee Management and Training

During employee orientation, each new employee will receive a copy of all current privacy policies, policies regarding non-disclosure of confidential information and trade secrets, information security programs and identity theft prevention programs and be trained regarding the importance of confidentiality of Personal Data. Training will include: (i) all policies and programs and the obligation to comply with such policies and programs, (ii) proper use of computers and passwords, (iii) controls and procedures to ensure that employees only access appropriate information, (iv) controls to prevent employees from providing confidential information to unauthorized parties, and (v) proper disposal of Personal Data. Employees should receive any amendments to such policies and programs and re-training as appropriate.

When an employee ceases to be employed by the Dealership, he/she is required to turn in any keys, passwords, computers, hard drives, devices or other access mechanisms in his/her possession. In addition, any security codes or passwords to which such employee had access will be changed or removed. Employees will not be permitted to take any Personal Data with them when their employment ceases.

Customer Information Collection

Customer information may be collected through a variety of collection methods including verbally, in writing, or via electronic means including transmission via the internet, e-mail, text message, wirelessly from connected equipment or hardware, or through third party access portals. Collection of Personal Data through any of these sources is covered by this program. When Personal Data is collected electronically, we will maintain appropriate security protocols, which may include encrypting information while at rest and/or in wireless transmissions.

Customer Identity Verification

The following procedures will be implemented with respect to customer identity verification from customer information:

- Forms used by the Dealership request certain 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.
- Employees may 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 may 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 may be required to provide employment information and references and may be required to authorize the Dealership to obtain a credit report, all of which may be used to verify the identity of the customer.
- 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 any applicable federal and state laws.

Information Security Safeguards

The following information security standards will be implemented in order to appropriately safeguard Personal Data collected and maintained by our Dealership:

- Employees are only authorized to have access to the Personal Data necessary to complete their responsibilities. Employees shall not access or provide any other unauthorized person access to Personal Data. Requests for Personal Data 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.
- Access to electronic Personal Data will be protected by a password or equivalent protection. Every employee with access to the Dealership's computer system, electronic devices and electronic records will have a unique password consisting of at least 8 characters and must include both numbers and letters. Employees will be instructed to not share their password with others or post or save their passwords in locations that are accessible to others in the Dealership or otherwise. After multiple failed login attempts from a single device or user, additional login attempts may be restricted.
- All paper and electronic records will be stored in secure locations to which only authorized employees will have access. Electronic Personal Data will be stored on a secure server that is located in a locked room and is accessible only with a password or key. Any remote access to Personal Data shall be conducted in a secure manner using a minimum of 128 bit encryption or other similar technology. Paper records will be stored in an office, desk, or cabinet that is locked when unattended. Customers, vendors and service providers shall not be left in areas with access to unsecured Personal Data.
- Backups of the computers and/or server will be made at regular intervals as deemed necessary. Virus protection software will be installed on computers and new virus updates will be checked at regular intervals. Firewalls and security patches from software vendors will be downloaded on a regular basis.
- All Personal Data will be erased from computers, disks, hard drives or any other electronic media that contain Personal Data before disposing of them. Any paper records will be shredded and disposed of securely.
- Employees will be instructed to log off of all internet, e-mail, social media or other accounts when they are not being used. Employees will be trained to not download any software or applications to Dealership computers or open e-mail attachments from unknown sources. Employees will be instructed to not download, upload, or save electronic records to external media or an individual's computer without explicit authorization from the Program Coordinator. If electronic records will be transmitted or accessed over an external network, including the internet, employees will be instructed to not use unprotected public Wi-Fi networks for such activities.

Service Provider Selection and Review

In order to protect the Personal Data our Dealership collects, we will take reasonable steps to initially select and then oversee our service providers that routinely access or utilize Personal Data. The following evaluation criteria may be utilized in selecting service providers:

- Compatibility and willingness to comply with the Dealership's privacy policies, information security program, and identity theft prevention program, as applicable.
- Adequacy of the service provider's own privacy policies and information security standards.

- Experience and ability to provide the necessary services and supporting technology for current and anticipated needs, which may include an evaluation of the service provider's knowledge and understanding of laws and regulations that are relevant to the services and information being provided.
- Financial stability of the service provider and reputation with industry groups, trade associations and other dealerships.
- Contractual obligations and requirements, which, among other legal and business term considerations, include requirements to implement and maintain appropriate security safeguards, maintain the confidentiality of Personal Data, only use Personal Data for purposes of providing services under the contract and reporting breaches to the Dealership.

Response to Breaches and Other 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 and Data Policy and Information Security Program and applicable law.

If the Dealership's Privacy and Data Policy or Information Security Program is breached, the Program Coordinator will assess the breach and determine whether notification to any parties is advisable or required by applicable law. To the extent determined to be advisable or required by law by the Program Coordinator, he/she will take appropriate steps to notify counsel, service providers and customers, as applicable, of any breach, damage or loss of information and the risks associated with the same. Further, as determined to be appropriate by the Program Coordinator based upon the breach and circumstances surrounding such breach, the Program Coordinator will 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 Privacy and Data Policy and Information Security Program, subject to any required Dealership approval.

General; Review

This Information Security Program was adopted and approved by Jeff Brakke – Dealer Principal & Jeff Paullus – General Manager on **12-30-13**. This Information Security Program will be reviewed at least annually by the Program Coordinator to assess its level of appropriateness for our Dealership.

I, THE UNDERSIGNED EMPLOYEE OF THE COMPANY, HAVE RECEIVED, READ AND UNDERSTAND THE ATTACHED INFORMATION SECURITY PROGRAM AND HAVE PARTICIPATED IN TRAINING REGARDING THE COMPANY'S INFORMATION SECURITY AND IDENTITY THEFT PREVENTION PROGRAMS.

_____

(Employee signature) (Date)

_____

(Employee name – printed)

A signed copy of this form will be placed in the employee's personnel file.