Klaben Automotive Group, Inc. Information Security Program (Employee Summary)

Drafted/Adopted: May 15, 2003
Reviewed/Updated by Legal & Management: January 1, 2018

Introduction
Klaben Automotive Group, Inc. and its automotive dealerships, Klaben Ford Lincoln, Inc., Klaben Ford Lincoln of Warren, Inc. and Klaben Chrysler Jeep Dodge, Inc. (each Dealership is herein referred to as a "Dealership", and collectively, "Klaben") are or may be considered "financial institutions" under the GLB Act and must comply with the provisions of the Act.

Company Policy and Program Objectives
It is the policy of Klaben to comply with the provisions of the Safeguards Rule of the GLB Act. Klaben and its employees will not intentionally share or disclose, or cause to be shared or disclosed, any customer information to any person or entity except where necessary to complete a financial transaction as authorized by the customer. Klaben and its employees will at all times strive to protect and secure all customer information that may be received during the course of a business transaction. Customer information may not be removed from the premises of Klaben without a legitimate business purpose.

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

- Insure the security and confidentiality of Klaben's customer information.
- Protect against any anticipated threats or hazards to the security and/or integrity of the Klaben's customer information.
- Protect against unauthorized access to or use of Klaben'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 any Dealership, or information any Dealership receives about the customer of another financial institution that can be directly or indirectly attributed to the customer.
This Program, in and of itself, does not create a contract between Klaben and any person or entity. This document summarizes the Information Security Program which outlines how "Klaben" and its employees intend to comply with the Act.

Program Coordinator(s)
This Program and the safeguards it contemplates shall be implemented and maintained by certain employees ("Program Coordinators") designated by the Klaben Automotive Group, Inc. and each Dealership. The Program Coordinators shall design, implement and maintain new safeguards as he or she determines to be necessary from time to time. Each Dealership Program Coordinator will report to the President of the Klaben Automotive Group, Inc.

Risk Assessment
Each Dealership Program Coordinator shall conduct a risk assessment 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.

Overseeing Service Providers
The Program Coordinators shall be responsible for overseeing the Dealership's service providers who handle or have access to customer information. The Program Coordinators 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.

The Program Coordinators shall review and approve each service provider contract prior to its execution by a Dealership to ensure that each contract contains appropriate obligations of the service provider to comply with the Dealership's safeguarding requirements.

Information Security Policies and Procedures – Information Systems
The Dealership shall take appropriate steps to encourage awareness of, and compliance with, the Program.
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.
    - Inactive paper records, such as completed deal files, shall be secured in rooms that are either locked or subject to controlled access in non-public areas.
    - Active paper records, such as deals in process, shall be stored in locked files or otherwise secured in non-public areas.
    - Electronic customer information shall be stored on secure servers. Access to such information shall be password controlled, and the Dealership Program Coordinator shall control access to such servers.
    - Customer information consisting of financial or other similar information (e.g., social security numbers, etc.) shall not be stored on any computer system with an unprotected internet connection.
    - Customer information will be backed up as part of our complete daily computer file back up process. Such back up data shall be stored in a secure location as determined by the Dealership Program Coordinators.
2. All electronic transmissions of customer information, whether inbound or outbound, shall be performed on a secure basis.
    - The Dealership shall require that inbound transmissions of customer information be delivered to the Dealership in a secure manner acceptable to the Dealership Program Coordinators.
    - All outbound transmissions of customer information shall be secured in a manner acceptable to the Dealership Program Coordinators.
    - 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 Dealership Program Coordinators.

- The Dealership Program Coordinator 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.

3. All paper transmissions of customer information by the Dealership shall be performed on a secure basis.
   - Sensitive customer information shall be secured at all times.
   - Customer information delivered by the Dealership to third parties shall be transported in a secure manner by being sealed in a delivery company provided container or personally delivered by a Dealership employee.
   - Paper-based customer information shall not be left unattended at any time that it is in an unsecured area.
4. All customer information will be disposed of in a secure manner.
   - Each Dealership Program Coordinator shall supervise the disposal of all bulk stored records containing customer information.
   - Paper based customer information shall be shredded as the preferred means of disposal after any applicable retention period has expired.
   - 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 will be effectively destroyed.
5. Each Dealership Program Coordinator shall maintain an inventory of Dealership computers, including any handheld devices or PDAs, on or through which customer information may be stored, accessed or transmitted.
6. All employees and independent contractors will be permitted to access customer information on a "need-to-know" basis as determined by Dealership management.
7. 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.
8. 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 and contract termination for independent contractors that perform services for the Dealership.

It is very important that we all work together to ensure our customer's information is handled, stored and processed in a secure manner. We all have an important role in this process. Please notify your supervisor or one of the Program Coordinator's listed below if you have any concerns about how information is being secured.

This is an "Employee Summary" of the "Information Security Program". The Program in its entirety can be found in the employee section of www.klaben.com, or you may request a paper copy from one of the Program Coordinators or your manager.

This program in and of itself, does not create a contract between Klaben and any person or entity.

Program Coordinators:

Program Coordinator	Heather Knapp	330-673-3139
Program Coordinator	Tracy Tucci	330-673-3139
Program Coordinator	Vicki Filipovich	330-369-4444
Program Coordinator	Carla Caskey	330-677-2888