Information Security Program (ISP)

Last Updated: Jul 13, 2023

1. Scope & Objectives

The objectives of this comprehensive written Information Security Program ("**ISP**") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Germain Automotive Partnership has selected to protect the personal information it collects, receives, uses, and maintains. All employees, staff, contractors, and guests of the following locations are expected to comply with this ISP:

- Germain Volkswagen
- Your Ride
- Germain Lincoln of Naples
- Toyota West
- Germain Lexus of Ann Arbor
- Germain Hyundai of Columbus
- Germain Subaru of Columbus
- Germain Nissan
- Germain Toyota of Naples
- Germain Kia of Columbus
- Germain Spartan Toyota
- Germain Mazda of Columbus
- Germain Ford
- Germain Toyota of Dundee
- Germain Mazda West
- Germain Lexus of Easton
- Germain Lexus of Dublin

All locations shall protect customer information by adopting and implementing, at a minimum, the security standards, policies, and procedures outlined in this ISP. This ISP outlines the minimum standards for the protection of personal information and each location is encouraged to adopt standards that exceed the requirements outlined in this ISP. This ISP has been developed in accordance with the requirements of all applicable state and federal laws, including, but not limited

to, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. §§ 314.1 to 314.5). If this ISP conflicts with any legal obligation or other Germain Automotive Partnership policy or procedure, the provisions of this ISP shall govern.

The purpose of this ISP is to:

- Ensure the security, confidentiality, integrity, and availability of personal information Germain Automotive Partnership collects, receives, uses, and maintains.
- Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
- Protect against unauthorized access to or use of Germain Automotive Partnership-maintained personal information that could result in substantial harm or inconvenience to any customer or employee. Fulfill Germain Automotive Partnership's obligation to comply with all state and federal regulations, policies, and standards associated with safeguarding customer information.
- Define an information security program that is appropriate to Germain Automotive Partnership's size, scope, and business, its available resources, and the amount of personal information that Germain Automotive Partnership owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

This ISP applies to all employees, contractors, officers, and directors of Germain Automotive Partnership. It applies to any records that contain personal information in any format and on any media, whether in electronic or paper form.

For purposes of this ISP, "**personal information**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer:

- Identifiers such as a real name, alias, postal address, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Customer records, including but not limited to, digital and electronic signatures, telephone numbers, insurance policy numbers, credit and debit card numbers, financial and credit-related information, physical characteristics and descriptions (e.g., government identification), bank account numbers, and medical and health insurance information (in the context of employment).
- Characteristics of protected classifications under state or federal law.
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Biometric information.
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
- Geolocation data.
- Audio, electronic, visual, thermal, olfactory, or similar information.
- Professional or employment-related information.

- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g, 34 C.F.R. Part 99).
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
- Persistent identifiers that can be used to recognize a consumer or a device that is linked to a consumer, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

"Personal information" does not include publicly available information, aggregate consumer information, or consumer information that is deidentified. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records.

2. Program Coordinator

This ISP and the safeguards it contemplates are implemented and maintained by a single qualified employee or service provider ("Program Coordinator") designated by Germain Automotive Partnership. The Program Coordinator is responsible for the design, implementation, and maintenance of information safeguards and other responsibilities as outlined in this ISP. The Program Coordinator may delegate or outsource the performance of any function under the ISP as he or she deems necessary from time to time. Germain Automotive Partnership has designated the following individual as the Program Coordinator:

- AJ Hall / IT Director / ahall@germain.com

The Program Coordinator shall be responsible for the following:

- Implementation and maintenance of this ISP, including, but not limited to:
  - Assessing internal and external risks to personal information and maintaining related documentation, including risk assessment reports and remediation steps;
  - Coordinating the development, distribution, and maintenance of information security policies and procedures;
  - Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal information;
  - Ensuring that the safeguards are implemented and maintained to protect personal information throughout Germain Automotive Partnership, where applicable;
  - Overseeing service providers, processors, and third parties that access or maintain personal information on behalf of Germain Automotive Partnership;

- Monitoring and testing the ISP's implementation and effectiveness on an ongoing basis through documented risk assessments and other mechanisms;
- Defining and managing incident response procedures; and
- Establishing and managing enforcement policies and procedures for this ISP, in collaboration with Germain Automotive Partnership's legal counsel, human resources department and upper management.

• Employee, staff, and contractor information security training, including:

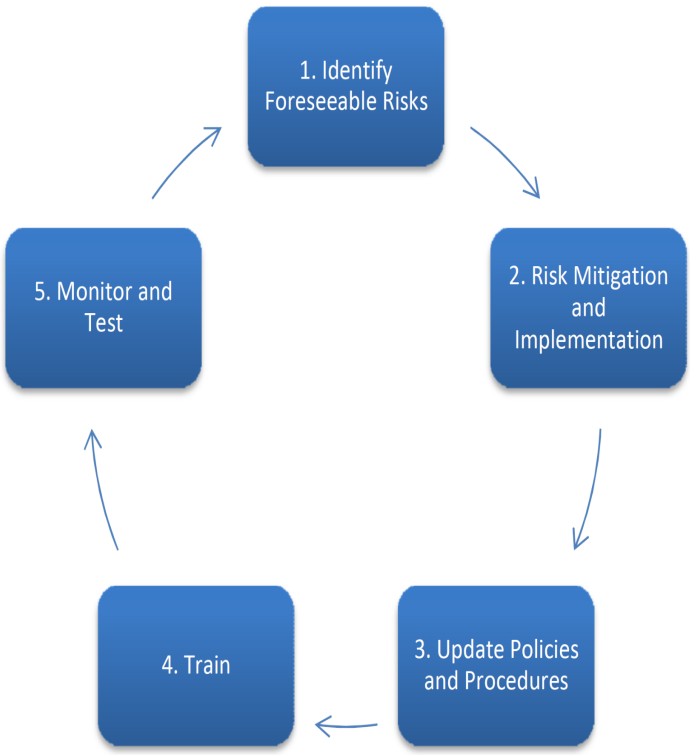
- Providing periodic security awareness and related training regarding this ISP, Germain Automotive Partnership's safeguards, and relevant information security policies and procedures for all employees, staff, and contractors;
- Ensuring that those employees, staff, and contractors who have been enrolled in training courses have completed and passed the course in a timely manner; and
- Retaining training completion records.

• Reviewing this ISP at least annually, or whenever there is a material change in Germain Automotive Partnership's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information.

• Periodically reporting to Germain Automotive Partnership management regarding the status of the information security program and Germain Automotive Partnership's safeguards to protect personal information.

3. Implementation Cycle

Germain Automotive Partnership utilizes a methodology that establishes information security policies based on periodic and updated risk assessments. Once initial risks are identified and assessed, mitigation controls are documented by the Program Coordinator or his/her designees. Employees are then trained and made aware of their responsibilities for following the proper information safeguards outlined in this document. Each Germain Automotive Partnership location will then be monitored and tested for its effectiveness at complying with the safeguards by performing updated risk assessments, performed at least annually. The process continues as periodic audits and risk assessments are conducted to identify and evaluate residual risk. The implementation cycle for this ISP is illustrated below.



4. Risk Assessments

As a part of developing and implementing this ISP, Germain Automotive Partnership, for each location, will conduct and document periodic risk assessments using the ComplyAuto Privacy electronic risk assessment tool, at least annually, or whenever there is a material change in Germain Automotive Partnership's business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal information.

The risk assessment shall evaluate:

- Reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal information;
- The likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal information; and
- The sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:
  - Employee, staff, and contractor, training and management;
  - Employee, staff, contractor, service provider, process, and third-party compliance with this ISP and related policies and procedures;
  - Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and
  - Germain Automotive Partnership's ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

Following each risk assessment, Germain Automotive Partnership will:

- Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks;
- Make available the results of the risk assessment to upper management for review;
- Reasonably and appropriately mitigate any identified risks or violations of this ISP and document such mitigation in the ComplyAuto Privacy online risk assessment tool; and
- Regularly monitor the effectiveness of Germain Automotive Partnership's safeguards, as specified in this ISP.

5. Safeguard Principals

Germain Automotive Partnership will develop, implement, and maintain reasonable administrative, electronic, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal information that Germain Automotive Partnership owns, accesses, or maintains on behalf of others. In doing so, Germain Automotive Partnership will adhere to the following principles:

- Safeguards shall be appropriate to Germain Automotive Partnership's size, scope, and business, its available resources, and the amount of personal information that Germain Automotive Partnership owns or maintains on behalf of others, while recognizing the need to protect both customer and employee personal information.
- Germain Automotive Partnership shall document its administrative, electronic, technical, and physical safeguards (see Section 6 of this ISP).
- Germain Automotive Partnership's administrative safeguards shall include, at a minimum:
  - Designating one or more employees to coordinate the information security program (see Section 2 of this ISP);
  - Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks (see Section 3 and 4 of this ISP);
  - Training employees in security program practices and procedures, with management oversight);
  - Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract (see Section 7 of this ISP); and
  - Adjusting the information security program in light of business changes or new circumstances.
- Germain Automotive Partnership's electronic and technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:
  - Secure user authentication protocols, including:
    - Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) or by using other technologies, such as biometrics or token devices;

  - Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and
  - Blocking a particular user identifier's access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
- Secure access control measures, including:
  - Restricting access to records and files containing personal information to those with a need to know to perform their duties; and
  - Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security.
- Encryption of all personal information traveling wirelessly or across public networks;
- Encryption of all personal information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal information stored on any other device or media (data-at-rest);
- Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal information or other attacks or system failures;
- Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal information; and
- Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software ("malware") definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

- Germain Automotive Partnership's physical safeguards shall, at a minimum, provide for:
  - Defining and implementing reasonable physical security measures to protect areas where personal information may be accessed, including reasonably restricting physical access and storing records containing personal information in locked facilities, areas, or containers;
  - Preventing, detecting, and responding to intrusions or unauthorized access to personal information, including during or after data collection, transportation, or disposal; and
  - Secure disposal or destruction of personal information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

6. Information Security Policies, Procedures & Safeguards

The following policies, procedures, and safeguards reflect Germain Automotive Partnership-'s objectives for managing operations and controlling activities related to information security. Additionally, the policies and procedures within this document represent Germain Automotive Partnership's ongoing efforts in achieving and maintaining internal control over customer information security as well as compliance with state and federal requirements. This section of the ISP outlines minimum requirements and is not meant to be a comprehensive or all inclusive list. The Program Coordinator shall implement, test, monitor, and enforce all of the policies and procedures covered below:

- General Dealership Safeguards

  - Documents with personal information shall not be left unattended on the desk or workspace of any employee. At a minimum, employees shall place any documents containing customer information in a drawer or enclosed container.

  - Customer personal information that is no longer part of an ongoing transaction (e.g., “dead” or “lost” deal documentation) should generally not be retained unless required by law or Germain Automotive Partnership policy, or unless it is securely stored, such in a locked drawer or file cabinet.

  - When away from their office, desk, or workspace, employees, staff, and contractors shall either (1) lock their office doors, or (2) utilize lockable storage for any customer personal information. If keys and/or locks are not available, then the workspace shall be cleared of all customer personal information, with no customer personal information left visibly unattended.

  - Files and documents containing personal information that do not need to be retained by state, federal, or internal Germain Automotive Partnership rules shall be securely destroyed and never placed into a regular trash or recycling bin. This includes mistakenly printed documents (including duplicates), as well as handwritten notes with customer personal information such as names, addresses, emails, and telephone numbers.

  - Printers, fax machines, copiers, and other office equipment shall be located in secure areas that are well monitored. At a minimum, documents should be immediately retrieved when faxed or printed from a remotely located machine. Under no circumstances should a document be left unattended at an unsecured machine location. Trash bins near copiers, printers, and other office equipment should be inspected for documents containing personal information.

  - Personal information should never be placed in a manner that exposes customer information to unintended individuals. When with a customer, only that customer’s personal information should be visible near the employee’s desk or workspace.

  - Credit application interviews, as well any other verbally communicated information involving the collection or disclosure of personal information, shall be conducted in areas secure from eavesdropping. Employees shall not use speakerphones in open areas susceptible to eavesdropping.

  - All new employees should be trained on the basics of customer information security policies, procedures and safeguards outlined in this ISP. This should be conducted during, and incorporated into, the new employee onboarding process. At a minimum, all employees shall be enrolled in the ComplyAuto Privacy “Dealership Security Awareness” and "Privacy and Information Security" courses or training program including similar content. Training shall recur, at a minimum, annually for each employee.

  - All employees shall be granted access to customer information (in both physical and electronic form) on a need-to-know and least-access basis. This shall include a process that restricts the ability to request or view deal jackets, repair orders, and other customer files to authorized individuals with a verified business purpose.

  - Germain Automotive Partnership shall conduct an inventory of all categories of personal information collected, map to which departments it is shared, the business purposes for which it is shared or disclosed, the categories of third parties and service providers to whom it is shared or disclosed, and the categories of sources from whom it is collected.

  - Germain Automotive Partnership shall maintain an up-to-date inventory of all enterprise assets, systems and devices with the potential to store or process personal information.

- Employees shall keep safety standard in place when data in en route. For example, when sending files containing personal information (e.g., mailing an F&I document to a customer for a missing signature), always use overnight shipping that lets you track where the package is. When there's a legitimate business need to travel with confidential information, employees shall keep it out of sight and under lock and key whenever possible. This also applies to electronic media in transit, such as drives, disks, devices, etc.

- Employees shall use and share only fictitious or test data (not real customer information) for training, development, or testing purposes. For example, when conducting sales, finance, or compliance training, employees shall either redact or use fictitious test data with respect to personal information. This also applies to printing out test documents, such as in the DMS to test contract and form alignment issues.

- Physical & Administrative Safeguards

  - Germain Automotive Partnership recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the physical and administrative safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, Germain Automotive Partnership shall do each of the following:

    - Protect File Storage Areas with Locking or Continuous Monitoring
    - Inspect Copiers and Office Equipment for Unattended Personal Information
    - Take Reasonable Steps to Protect File Storage Areas From Destruction and Damage
    - Ensure Computers Are Not Left Unlocked and Verify Automatic Session Locking is Working as Intended
    - Inspect for Improper Disposal of Customer Information
    - Provide Mechanisms for Secure Disposal of Personal Information
    - Inspect Employee Workspaces for Unattended Personal Information & Security Credentials

- Electronic & Technical Safeguards

  - Germain Automotive Partnership recognizes that best practices relating to information security are constantly evolving and therefore adopts many of the technical safeguards outlined in guidance and enforcement actions from the Federal Trade Commission. Accordingly, Germain Automotive Partnership shall do each of the following:

    - Electronic Data Containing NPI is Securely Deleted Upon Expiration of Legal and Business Need
    - Limit Administrative Access to a Neutral Department or Person
    - Require Complex and Unique Passwords on All Workstations and Applications
    - Prohibit the Practice of Storing User Credentials and Password in Vulnerable Formats
    - Protect Against Brute-Force Attacks for Local Devices & Web Applications
    - Encrypt Data at Rest and in Transit
    - Use Firewalls, VLANs, or Equivalent Methods to Segment Networks
    - Install EDR Software and Continuously Monitor Logs on All Endpoints
    - Require Remote Network Access Be Done Through VPN and MFA, or an Equivalently Secure Method.
    - Place Limits on Third-Party Access to Networks and Applications

- Update and Patch Operating Systems & Applicable Third-Party Software
- Encrypt Data Sent Over Point-of-Sale Devices
- Use Application Allow-Listing to Restrict Installation & Running of Unauthorized Software
- Encrypt Information Sent Over Wireless Networks
- Ensure Digital Copiers Have Encryption, Overwriting, Auto-Wiping Enabled
- Add Auto-Wiping, Encryption, or Centralized Computing to Mobile Devices
- Configure Automatic Session Locking on Workstations & Devices
- Enable MFA for All Company Email Accounts & Identity Services
- Enable MFA for All Third-Party Cloud-Based Applications Containing NPI
- Enable MFA for Employee Workstations and Internal Servers Containing NPI
- Perform Automated Backups of Sensitive Data That Are Kept Segregated or Offline
- Implement Controls to Monitor and Log Unauthorized Employee Use of Customer Information

- Adoption of Safeguards under the CIS Controls Framework

  - Germain Automotive Partnership also adopts the physical, administrative, and technical safeguards outlined in version 8 of the Center for Internet Security (CIS) Controls. Accordingly, Germain Automotive Partnership shall do each of the following:

    - Establish and Maintain Detailed Enterprise Asset Inventory
    - Address Unauthorized Assets
    - Establish and Maintain a Software Inventory
    - Ensure Authorized Software is Currently Supported
    - Address Unauthorized Software
    - Establish and Maintain a Data Management Process
    - Establish and Maintain a Data Inventory
    - Configure Data Access Control Lists
    - Enforce Data Retention
    - Securely Dispose of Data
    - Encrypt Data on End-User Devices
    - Establish and Maintain a Secure Configuration Process
    - Establish and Maintain a Secure Configuration Process for Network Infrastructure
    - Configure Automatic Session Locking on Enterprise Assets
    - Securely Manage Enterprise Assets and Software
    - Manage Default Accounts on Enterprise Assets and Software
    - Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
    - Establish and Maintain an Inventory of Accounts
    - Use Unique Passwords
    - Disable Dormant Accounts

- Establish an Access Granting Process
- Establish an Access Revoking Process
- Require MFA for Remote Network Access
- Require MFA for Administrative Access
- Establish and Maintain a Vulnerability Management Process
- Establish and Maintain a Remediation Process
- Perform Automated Operating System Patch Management
- Perform Automated Application Patch Management
- Establish and Maintain an Audit Log Management Process
- Ensure Use of Only Fully Supported Browsers and Email Clients
- Deploy and Maintain Anti-Malware Software
- Configure Automatic Anti-Malware Signature Updates
- Ensure Network Infrastructure is Up-to-Date
- Establish and Maintain a Security Awareness Program
- Train Workforce Members to Recognize Social Engineering Attacks
- Train Workforce Members on Authentication Best Practices
- Train Workforce on Data Handling Best Practices
- Train Workforce Members on Causes of Unintentional Data Exposure
- Train Workforce Members on Recognizing and Reporting Security Incidents
- Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
- Establish and Maintain an Inventory of Service Providers
- Designate Personnel to Manage Incident Handling
- Establish and Maintain Contact Information for Reporting Security Incidents
- Establish and Maintain an Enterprise Process for Reporting Incidents

- Record Request & Information Disclosure Policies

  - Only authorized employees shall disclose, share, send, or provide customer personal information to third parties.

  - In general, customer records containing personal information should not be mailed, emailed, texted, faxed, or otherwise transmitted electronically. Whenever possible, employees authorized to provide customer records containing personal information shall require the customer to pick up the records in-person after being required to present a valid government-issued photo identification. If the person cannot reasonably be expected to visit the dealership, the person's identity must be verified using both of the following methods:

    - Requesting they fax a copy of a valid government-issued photo identification;

- In the event a customer prefers to email or text their license, employees have an obligation to inform the customer that Germain Automotive Partnership DOES NOT endorse, recommend or request sensitive information be sent via email. Furthermore, employees are prohibited from accepting such information in the form of a text, whether on a company or personal phone. A customer who insists on sending information via email should be informed of the risks of sending information over an unencrypted network and that faxing or coming in person are safer alternatives.

• Requesting the person's full name and at least two other identifiers such as date of birth, address, phone number, last four digits of Social Security Number, email address, VIN, or name of the salesperson who assisted them.

- Germain Automotive Partnership personnel handling record requests have an obligation to securely destroy and shred customer information obtained in the process of verifying a customer's identity (e.g. shredding a faxed government-issued photo ID).

- In no event may documents containing sensitive customer information (e.g., financial information, Social Security Number, credit information, and identification cards) be mailed or electronically transmitted. Customers must retrieve such documents from the dealership in-person after presenting a valid government-issued photo identification.

- To the extent possible and reasonable under the circumstances, sensitive information should be redacted from files prior to them being released to the customer.

- Unless required by state or federal law, under no circumstance shall a DMV Registration Inquiry Report ("KSR" or similar report from a state motor vehicle department) or Consumer Credit Report be provided to a customer or other third party.

- In regard to service records, a customer is only entitled to records related to the period for which he/she was the owner of the vehicle in question. Employees have an obligation to review service records prior to release in order to ensure the customer is only getting information pertaining to his/her period of ownership.

- In general, customer records containing personal information should not be provided to unaffiliated third parties (e.g., vendors, manufacturers, and financial institutions) unless doing so is (1) required by law, (2) required to process a transaction initiated or requested by the consumer or (3) pursuant to a valid subpoena.

- Special rules under state and federal laws govern the disclosure of information related to victims or potential victims of identity theft. Employees should contact competent legal counsel regarding requests related to identity theft.

7. Service Provider Oversight

Germain Automotive Partnership will oversee each of its service providers and processor that may have access to or otherwise create, collect, use, or maintain personal information on its behalf by:

• Evaluating the service provider's or processor's ability to implement and maintain appropriate security measures, consistent with this ISP and all applicable laws and Germain Automotive Partnership's obligations. This may include having the service provider or processor complete a ComplyAuto Privacy electronic vendor risk assessment.

- Requiring the service provider or processor by contract to implement and maintain reasonable security measures, consistent with this ISP and all applicable laws and Germain Automotive Partnership's obligations. This may include having the service provider or processor complete and sign an applicable Data Processor Agreement in the ComplyAuto Privacy software.
- Monitoring and auditing the service provider's or processor's performance to verify compliance with this ISP and all applicable laws and Germain Automotive Partnership's obligations.

8. IT Change Management Policy

Changes to Germain Automotive Partnership's IT infrastructure introduces a heightened risk of cybersecurity incidents. Accordingly, this section governs the addition, removal, or modification of the elements of Germain Automotive Partnership's IT infrastructure as follows:

- **Adding and removing end-user devices**. The Program Coordinator or designated IT personnel must be involved in adding end-user devices. Adding end-user devices, such as desktops, laptops, phones, or tablets requires that the devices be securely configured in accordance with the technical and electronic safeguards outlined in this policy. This includes, but is not limited to, automatic session locking after a defined period of inactivity, strong password requirements, and device lockouts after a number of failed authentication attempts. If possible, portable devices should be set up to support remote wiping of all company data upon suspected theft, loss, or employee termination.
- **Adding third-party software & applications**. Prior to adding any third party software or applications (whether hosted on premises or cloud-based), the vendor must be assessed for the adequacy of their technical and physical information safeguards. This includes, at a minimum, completing an electronic vendor risk assessment questionnaire in the ComplyAuto system.
- **Additions or modifications to web browsers**. Cybercriminals can exploit web browsers in multiple ways. If they have access to exploits of vulnerable browsers, they can craft malicious webpages that can exploit those vulnerabilities when browsed with an insecure, or unpatched, browser. Alternatively, they can try to target any number of common web browser third-party plugins that may allow them to hook into the browser or even directly into the operating system or application. Accordingly, before allowing any browser to execute on the network, the following must be ensured:
  - Browser plugins are limited to trusted sources or otherwise disabled. Many plugins come from untrusted sources, and some are even written to be malicious. Therefore, it is best to prevent users from intentionally or unintentionally installing untrusted plugins that might contain malware or critical security vulnerabilities.
  - Automatic updates and patches for the browser and plugins have been properly configured.
  - Content filters for phishing and malware sites have been enabled.
  - Pop-up blockers have been enabled. Pop-ups can host embedded malware directly or lure users into clicking links using social engineering tricks.

- **Major additions or modifications to servers, operating systems, or network elements**. Any major modification, addition, or removal of servers, operating systems, or network elements (e.g., routers, switches, and firewalls) must be accompanied by the following:
  - A full internal penetration test.
  - A full internal and external vulnerability assessment.
  - A full configuration scan using a tool such the CIS-CAT Pro Assessor available from ComplyAuto.
  - Consider conducting a technical risk assessment in ComplyAuto that is designed to assess the safeguards outlined in this Program, as appropriate based on the changes made.

9. Data Retention Plan

The information of Germain Automotive Partnership is important to how it conducts business, protects customer data, and manages employees. Federal and state law require Germain Automotive Partnership to retain certain customer records, usually for a specific amount of time. Germain Automotive Partnership must retain certain records because they contain information that (1) serves as Germain Automotive Partnership's corporate memory, (2) have enduring business value, or (3) must be kept to satisfy legal, accounting, or regulatory requirements. The accidental or intentional destruction of these records during their specified retention periods could result in the following consequences for Germain Automotive Partnership and/or its employees:

- Fines and penalties.
- Loss of rights.
- Obstruction of justice charges.
- Inference of spoliation of evidence and spoliation tort claims.
- Contempt of court charges.
- Serious disadvantages in litigation.

This policy is part of a company-wide system for the review, retention, and destruction of records Germain Automotive Partnership creates or receives in connection with the business it conducts. Any type of information created, received, or transmitted in the transaction of Germain Automotive Partnership's business, regardless of physical format (collectively “record” or “records” hereinafter) are covered by this policy. Examples of where the various types of information are located include:

- Appointment books and calendars.
- Audio and video recordings.
- Computer programs and online applications.
- Contracts.
- Deal files.

- Electronic files.
- Emails.
- Handwritten notes.
- Hard drives.
- Invoices.
- Letters and other correspondence.
- Memory in cell phones and mobile devices.
- Online postings, such as on Facebook, Twitter, Instagram, Snapchat, Slack, Reddit, and other social media platforms and websites.
- Repair files.
- Voicemails.

Therefore, any paper records and electronic files that are part of any of the categories listed in the Records Retention Schedule contained in this policy, must be retained for the amount of time indicated in the Records Retention Schedule. A record must not be retained beyond the period indicated in the Record Retention Schedule, unless a valid business reason (or a litigation hold or other special situation) calls for its continued retention. If you are unsure whether to retain a certain record, contact the Program Coordinator or legal counsel.

Germain Automotive Partnership prohibits the inappropriate destruction of any records, files, documents, samples, and other forms of information. Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose and/or data that may be safely destroyed because it is not a record as defined by this policy. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of Germain Automotive Partnership and retained primarily for reference purposes.
- Spam and junk mail.

How and When to Destroy Records

Germain Automotive Partnership's Program Coordinator is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction. Regarding customer information, if no record retention period is specified, the secure disposal of customer information in any format must occur no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes. The destruction of confidential, financial, customer and personnel-related records must be conducted by shredding. The destruction of electronic records must be coordinated with the Program Coordinator. The destruction of records must stop immediately upon notification from legal counsel that a litigation hold is to begin because

Germain Automotive Partnership may be involved in a lawsuit or an official investigation (see below). Destruction may begin again once legal counsel lifts the relevant litigation hold.

Litigation Holds and Other Special Situations

Germain Automotive Partnership requires all employees to comply fully with its published records retention schedule and procedures as provided in this policy. All employees should note the following general exception to any stated destruction schedule: If you believe, or legal counsel informs you, that Germain Automotive Partnership records are relevant to current litigation, potential litigation (that is, a dispute that could result in litigation), government investigation, audit, or other event, you must preserve and not delete, dispose, destroy, or change those records, including emails, until legal counsel determines those records are no longer needed. This exception is referred to as a litigation hold or legal hold and replaces any previously or subsequently established destruction schedule for those records. If you believe this exception may apply, or have any questions regarding whether it may possibly apply, please contact legal counsel. In addition, you may be asked to suspend any routine document disposal procedures in connection with certain other types of events, such as the merger of Germain Automotive Partnership with another organization or the replacement of Germain Automotive Partnership's information technology systems.

Periodic Review & Other Responsibilities

The Program Coordinator shall periodically review this policy and its procedures with legal counsel and/or Germain Automotive Partnership's certified public accountant to ensure Germain Automotive Partnership is minimizing the unnecessary retention of data to the extent possible and is in full compliance with relevant new or amended regulations. The Program Coordinator (or a more qualified individual as determined by the Program Coordinator) is responsible for identifying the documents that Germain Automotive Partnership must or should retain, and determining, in collaboration with legal counsel, the proper period of retention. The Program Coordinator also arranges for the proper storage and retrieval of records, coordinating with outside vendors where appropriate. Additionally, the Program Coordinator is responsible for the destruction of records whose retention period has expired.

Record Retention Schedule

Occasionally Germain Automotive Partnership establishes retention or destruction schedules or procedures for specific categories of records. This is done to ensure legal compliance and accomplish other objectives, such as protecting intellectual property and controlling costs. Employees should give special consideration to the categories of documents listed in the record retention schedule below. Avoid retaining a record if there is no business reason for doing so, and consult with the Program Coordinator or legal counsel if unsure.

ACCOUNTING / TAX INFORMATION	
Cash books and receipts	7 years
Canceled checks	10 years

Credit cards and other merchant transaction records	6 years
Credit memos	6 years
IRS Form 8300 filings	5 years
Report of sales books	8 years

DEALERSHIP OPERATIONS	
Credit applications (and all related documents) in situations where a sale is made	7 years
Credit applications (and all related documents) in situations where no sale was made	25 months
Deal jackets and associated customer files: vehicle contracts and leases, service contracts, buyers guide (if applicable).	7 years
Demo vehicle agreement and related records	6 years
Email regarding topics in this chart	The applicable topic
Emails not regarding topics in this chart	6 months after creation
Odometer disclosures, including copy of odometer disclosures on title and related Power of Attorney documents	5 years
Vehicle registration documentation	6 years
Report of sales documents	8 years
Rental agreements	7 years
Telemarketing: Advertising, brochures, scripts, promo materials	2 years
Telemarketing: Name and address of prize winners valued $25 or more	2 years
Telemarketing: Name and address of customer, goods/services purchased, date, amount paid	2 years
Telemarketing: Verifiable authorizations or records or express informed consent or express agreement required to be provided under this Rule	2 years
Telemarketing: Compliance materials (do-not-call records, etc.)	9 years
Service contracts and extended warranties	10 years
Accident Records	1 year
TILA "evidence of compliance" statements	2 years

FIXED OPERATIONS	
Customer repair orders	4 years
Over-the-counter parts invoices and parts sales slips	6 years
Towing records	3 years
Data collected when duplicating keys	2 years

INSURANCE RECORDS	
Incident reports prepared for insurance claims	6 years
Claims register, or other records that proves whether or not a claim was received	10 years
Claims in Occurrence-based Policies	6 years
Claims in Claims-based Policies	6 years

LEGAL RECORDS	
Data breach notifications to consumers	Permanently
Data Subject / Privacy Requests and responses (CCPA, CPRA)	2 years
Lawsuit files	Permanently
Express written consent for TCPA (from consumers to contact via phone, text message, etc.)	Permanently
Telemarketing compliance materials (internal do-not-call records, national do-not-call downloads, etc.)	2 years

10. Enforcement

Violations of this ISP may result in disciplinary action, up to and including termination, in accordance with Germain Automotive Partnership's human resources policies. Disciplinary actions will be documented in response to violations identified in the ComplyAuto Privacy online risk assessment tool.

11. Program Review

Germain Automotive Partnership will review this ISP and the security measures defined herein at least annually, or whenever there is a material change in Germain Automotive Partnership-'s business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal information. Germain Automotive Partnership shall retain documentation regarding any such program review, including risk assessment, mitigation steps, disciplinary actions, and remediatory actions.

12. Effective Date

This ISP is effective as of Mar 30, 2023 .