Written Information Security Program

Twin City Motors, Inc. and Twin City Classic Automotive, Inc.

1. Purpose and Objective

Twin City Motors, Inc. and Twin City Classic Automotive, Inc. (referred to herein as Twin City) will protect confidentiality, security and integrity of information entrusted to it. This Information Security Program provides administrative, technical, and physical safeguards for the protection of the confidentiality, security and integrity of Protected Information (as defined below), including personal information and confidential business information, against anticipated threats or hazards. It also protects the continuity of operations by providing for safeguards of Information Systems.

2. Scope

For purposes of this program, "Protected Information" includes

(i) Nonpublic personal information (as defined in the Gramm-Leach-Bliley Act)

(ii) Personal information (or similar terms) as defined by applicable law collected from and about job applicants, employees, officers, directors, contractors, and other representatives of Twin City

(iii) The proprietary or confidential information of Twin City

(iv) Proprietary or confidential information of third parties processed by Twin City and required by applicable law or contract to be protected (collectively referred to as "Protected Information")

"Information Systems" includes

(i) All systems used by Twin City to process "Protected Information"

(ii) All operating systems used in the operation of the business of Twin City, the disruption of which would be likely to have a material adverse effect on the operations of Twin City.

This Program applies to all users with access to Protected Information and Information Systems of Twin City.

3. Governance and Compliance

This Program and all associated policies and procedures must be reviewed at least annually by the CISO in order to evaluate potential threats and revise measures being taken to address those threats. This evaluation should include analysis of changes in relevant technology, sensitivity or information, changes in business operations or arrangements, and changes to the threat environment. Even if there are no changes to the document, a review revision must be added to the Document Change Log at the beginning of each document. All changes to this program recommended by the CISO must be submitted in writing and approved by the President. All submitted changes must include a description of why the change is necessary or advisable, and what other compliance components it may affect.

The CISO shall report to the Board of Directors no less frequently than annually. These reports shall include a review and assessment of the status and functioning of this Program and any recent revisions or improvements.

Each individual and entity with access to Nonpublic Information and Information Systems must comply with the applicable requirements of this Program.

Any violation or suspected violation of this program must be reported to the CISO.

Failure to comply with this Program may result in disciplinary action up to and including termination.

4. Program Communication

All Twin City employees must read and acknowledge this Program at least annually. All new employees must read and acknowledge this Program at time of hire. This Program will be located on the Twin City Employee website so that all employees may view and download. It is the responsibility of the CISO to convey the location of this Program and ensure that all personnel involved with information systems and data handling have read and acknowledged this Program. In addition, as discussed below, policies will be established to require personnel to undergo training with respect to information security practices appropriate to their respective roles within Twin City.

5. Exceptions to Program

Any exceptions to the requirements of this Program must be approved in advance by the President. Each approval must be documented in writing, together with the justifications therefore, and any compensating considerations or remedial requirements.

6. Organizational and Functional Responsibilities

The CISO is the senior officer responsible for developing, implementing, reviewing, and updating this Program.

7. Data Classification

All Protected Information must be protected from unauthorized access to maintain the confidentiality and integrity of the information. Protected Information generated and maintained by Twin City has varying degrees of security sensitivity depending on the nature and the use of the data. All information (including Protected Information) must be classified by the department manager and approved by the CISO as either **restricted**, **confidential**, or **public**, so that the appropriate security measures are taken with respect to such information. All questions concerning data classification will be referred to the CISO. **See Appendix A, *Examples of Protected Information.***

8. Risk Assessment

Twin City shall conduct a risk assessment no less frequently than annually, and at such additional times as may be deemed appropriate by the CISO, to identify the potential risks to and vulnerabilities of Protected Information and Information Systems. Based on the risk assessment, Twin City shall further adopt and implement reasonable and appropriate administrative, technical and physical safeguards to protect against reasonably foreseeable threats to the confidentiality, integrity and availability of the Protected Information and the Information Systems. The CISO shall report promptly to the President the results of each risk assessment, and related recommendations for safeguard enhancements.

9. Data and Systems Protection

All Protected Information and Information Systems must be protected against all known threats, unauthorized access, mishap, and/or accidental leakage commensurate with the appropriate classification level, and all other compliance requirements. Applicable legal and contractual requirements obligate Twin City to encrypt certain information during transmission, on mobile devices, and/or in storage, and Twin City has taken the approach of encrypting all information on all devices. All encryption technologies used by Twin City must be approved in advance by the CISO. Antivirus software approved by the CISO must be deployed to all applicable Information Systems to protect against malware and other software deviants. System patches must be reviewed, ranked, and deployed promptly. Information Systems may require specific monitoring and periodic testing commensurate with the sensitivity and criticality of the systems and the data processed, and other compliance requirements. Employees must receive training to understand the importance of locking computers when they are not in use and the proper use of Multi-Factor Authentication (MFA).

10. Protecting Encryption Keys

Encryption is ineffective if encryption keys or certificates are not secured. All encryption keys and/or certificates must be protected from unauthorized disclosure using industry standard technologies, procedures, and/or purpose-built security devices approved by the CISO.

11. Security Awareness Program

The CISO is responsible for the content and delivery of security awareness training and education. Security will be a topic of orientation of all new employees. All employees will be presented security awareness training at least annually, or more frequently as may be required by compliance programs. IT and security personnel will be provided targeted and specialized education relevant to their job functions. An acknowledgement of attendance and understanding must be obtained from each employee and retained by the appropriate department. The intent of the security awareness program is to educate employees on contemporary security issues and proper data and systems usage. As part of their security awareness training and education, IT and security personnel must review and acknowledge all IT security policies and this Program upon onboarding and annually thereafter.

12. Physical Security of Information Systems

Information Systems, including computers, peripherals, and all network components, must be secured against access by unauthorized persons, and against misuse, loss, theft, and natural disasters. The sensitivity of Protected Information and Information Systems requires appropriate controls over use of and access to those assets. Controls to deter and protect against theft or damage to equipment are also required.

13. Access Control

Nonpublic Information and Information Systems, including the physical locations where they are housed, must be protected against unauthorized access, misuse, and/or theft by restricting access to only the appropriate processes, technologies, and/or persons.

Physical information will be secured in locked filing systems, or in a locked storage room. Access authorization will be granted by the CISO.

MFA will be implemented anywhere there is company data. A Group Policy Object (GPO) policy will be implemented to disable external USB ports on all hardware unless authorized by the CISO.

14. Secure Disposal of Equipment and Sensitive Data

All equipment containing storage media (e.g., fixed hard disks) must be examined to ensure that any Protected Information and any licensed software are securely removed or overwritten prior to disposal.

Physical information will be placed in locked shred bins. Keys to the shred bins will be distributed to the department managers. A bonded and insured shredding company will be employed to appropriately destroy documents. **See Appendix B *Records Retention Schedule***.

Hard drives are to be removed from retired PC’s and destroyed. Technical information is to be stored in the IT GLUE platform and secured with MFA.

15. Network Security

Network connections will be granted access by IT personnel based on written, emailed, or help desk request from a department manager. Unusual or questionable requests will be referred to the CISO for authorization.

16. Wireless Networking

Wireless technologies will be deployed by IT Personnel only after all approvals, including the CISO and President have been completed. The IT Director will be responsible for assuring that "rogue" wireless devices are detected and eliminated.

17. Remote Access

Employees requiring remote access must be approved by the President. All access must be performed on Twin City approved equipment, software, communication lines, and procedures. Multi-factor authorization must be deployed to limit the risk of unauthorized access.

18. Internet Connectivity to Information Systems

Connections from the Internet to Information Systems will be installed by IT personnel based on written, emailed, or help desk request from a department manager. Unusual or questionable requests will be referred to the CISO for authorization.

19. Third-Party Vendor Management

All third-party vendors and service providers must be approved by the CISO in order to obtain access to Protected Information. They will be required to sign the security addendum or provide sufficient evidence of their specific company policies regarding the security of our customer information. The executed contract addendum and/or other approved documentation will be kept on file and reviewed or updated annually.

20. System User Provisioning

Strict control must be maintained over user account management. All users (including third party vendors) requesting access to Twin City systems or data must follow approved processes to obtain approval.

21. System Monitoring, Testing, and Risk Self-Assessment

All systems and data will be monitored and tested commensurate with classification levels, as determined from time to time by the IT Department.

22. Software Deployment

No software shall be developed, requisitioned, or deployed on any Information Systems without the prior written approval by the IT Director, after the completion of such due diligence and contracting as the IT Director may deem appropriate.

23. Incident Response

"Information Security Incident" means any actual or reasonably suspected compromise of the confidentiality, security or availability of Protected Information or Information Systems, including:

- (i) Unauthorized access, acquisition, use, disclosure, or transmission of Protected Information
- (ii) Loss, theft, or unauthorized destruction of Protected Information or Information Systems
- (iii) disruption or unauthorized use of Information Systems.

Any actual or suspected Information Security Incident shall be reported immediately to the CISO. The CISO shall conduct an appropriate investigation and take (or cause to be taken) all reasonable and appropriate measures to remediate the incident and determine the scope of the affected information and systems. The CISO must immediately report to the President any Information Security Incident reasonably determined or expected to be material in scope, cost or other effect. The CISO is responsible for notifying the appropriate insurance carrier, engaging outside resources to investigate and remediate the incident, and to advise Twin City as to its obligations under applicable legal and contractual requirements.

24. Disaster Recovery; Contingency Planning

See Appendix C, ***IT Business Continuity Plan*** for the management company SETCAII and affiliated dealerships.