**INCIDENT RESPONSE PLAN**

Classic-Tyler Motors, Inc.

**I. BACKGROUND, ORGANIZATION AND ROLES**

**1.0 Policy Statement; Overview**

It is the policy of Classic-Tyler Motors, Inc.,and Classic-Tyler Motors II, Inc., hereafter called Classic Tyler to respond to Security Incidents (defined below) in a timely and appropriate manner, and in compliance with applicable law. Security Incidents can come in many forms, such as a malicious attacker gaining access to the network, theft of a laptop containing Protected Information, inadvertently emailing Protected Information to an unauthorized recipient, or a loss of paper records containing Protected Information.

# 2.0 Purpose

The purpose of this Incident Response Plan is to assign roles and responsibilities, and to provide guidelines for responding to potential Security Incidents involving Classic Tyler Protected Information, or other Information Assets.

###  Scope

This Incident Response Plan ("'Response Plan") covers the response to Security Incidents that threaten the confidentiality, integrity, and availability of Classic Tyler Information Assets. It covers both paper and electronic Information Assets, and applies to Security Incidents of all types, whether they are the result of physical, environmental, technical, or human threats.

### 4.0 Objectives

The objectives of the Response Plan are to:

* + - Establish guidelines for identifying and responding to Security Incidents
		- Respond to Security Incidents systematically so that the appropriate steps are taken:
		- Help Classic Tyler to recover quickly and efficiently from Security Incidents, minimizing loss or theft of information, disruption of services and damage to the company
		- Deal properly with legal and policy issues that may arise during, or as a result of Security Incidents
		- Use information gained during Incident handling to better prepare for handling future Incidents and to provide stronger protection for Information Assets

**5.0 Updates and Approval**

This Response Plan is intended to be a living document and will be regularly (at least annually) reviewed and updated as appropriate. This Response Plan must be reviewed and approved by the Chief Information Security Officer (CISO), IT Director, and a Classic Tyler senior officer at least annually. The IT Director will first review the Response Plan, suggest changes, and present any revisions to the CISO for review. The Response Plan and any addenda, attachments or exhibits may also be updated from time to time as the IT Director, CISO,or other senior officer may deem necessary.

# 6.0 Related Documents

The following policies are related to this Response Plan and should be reviewed and coordinated with this Response Plan:

|  |  |
| --- | --- |
| **For policies on ……** | **See…..** |
| Document Destruction | *Information Security Program- Appendix B: Records Management and Document Retention Policy* |
| Maintaining system integrity and security | *Information Security Program* |
| Disaster recovery | *Information Security Program – Appendix C: Business Continuity Plan* |
|  |  |

# Definitions

The following definitions apply to this policy:

**“Protected Information"** means (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 Classic Tyler; (iii) the proprietary or confidential information of Classic Tyler; or (iv) proprietary or confidential information of third parties processed by Classic Tyler and required by applicable law or contract to be protected (collectively referred to as "Protected Information").

**"Incident''** -See “Security Incident”

**"Information Assets"** means the following technology and information assets of Classic Tyler:

* + - Computer hardware including hardware with processing or communications capabilities, such as servers, computers, PCs, laptops, tablets, routers, mobile phones, etc.; and storage media such as disks, tapes, DVDs, flash drives, etc.
		- System software including operating systems, database management systems, email software,

backup and restore software, communications protocols, and so forth.

* + - Application software used by the various departments within the company, including both custom written software applications and commercial off the shelf software packages
		- Communications network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools; and
		- Protected Information.

"**Information Systems**" includes (i) all systems used by Classic Tyler to process Protected Information; and (ii) all operating systems used in the operation of Classic Tyler, the disruption of which would be likely to have a material adverse effect on the operations of Classic Tyler

**"Third Partv Provider"** means any person or entity that maintains, processes, or otherwise is permitted access to Protected Information through its provision of services directly to Classic Tyler

**"Unauthorized Access"** means where Protected Information (whether Corporate Information, Customer

Information or Personal Information) maintained by or on behalf of Classic Tyler

is obtained, accessed or used by persons or entities that are not authorized, by law, contractor, other relationship with a Customer, or Classic Tyler to obtain, use or access such information.

**"Securitv Incident'' (or Incident)** means any actual 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; or (iii) disruption or unauthorized use of Information Systems.

### 8.0 Confidentiality of Security Incidents

All information related to a potential Security Incident must be treated as highly confidential unless otherwise

directed by the CISO. This will serve both to protect employees' reputations (if an incident is due to an error, negligence. or carelessness), and to control the release of information to the public.

### 9.0 Roles and Responsibilities, Generally

Each Classic Tyler employee has responsibilities related to the security of Classic Tyler’s computing systems and its Protected Information. All Classic Tyler employees are made aware of the procedures applicable to Security Incidents through annual compliance training.

**9.1 All Employees**

Users of Classic Tyler’s information, computers, and systems may be the first to discover an incident. Many Security Incidents are caused by authorized users of a company's system. Therefore, employees and other authorized users are Classic Tyler's first line of defense in detecting and possibly avoiding Security Incidents. Accordingly, both end users and technical personnel need to be vigilant in monitoring for unusual system behavior, which may indicate a Security Incident or other incident (e g., virus infections, system compromises, denial of service attacks, inadvertent transmission of Protected Information, etc.) in progress.

Any employee of Classic Tyler who is aware of or suspects that a Security Incident has occurred or is occurring (including at or with one of Classic Tyler's Third Party Providers) must immediately contact the He1pdesk at email *help@myclassictoyota.com,* or the IT Director at Phone: *(903) 330-3340;* or email *helpdesk@myclassictoyota.com.*

 **9.2 Security Incident Response Team**

The Security Incident Response Team **('Response Team")** has primary authority for responding to all potential Security Incidents, which includes the following:

* Validating that a Security Incident has occurred
* Managing the investigation and response to Security Incidents
* Managing the recovery and remediation process; and
* Working with various internal stakeholders and external consultants while managing the Security Incident response process

The members of the Response Team are listed on **Appendix A**

**Security Incident Response Team Roles and Responsibilities**

|  |  |
| --- | --- |
| Role | ·Responsibilities |
| **IT Director - (Response Team Leader)** | The IT Director will serve as leader of the Response Team. In this capacity, the IT Director will act as the coordinator for all Security Incidents, and will assign individuals to specific related tasks. The IT Director has the authority to commit company resources that are needed in responding to an incident. When necessary, the IT Director should escalate concerns and issues to the President and other executives. |
| CISO | The CISO will serve as the information technology point person responsible for assisting the IT Director in responding to potential Security Incidents. The CISO will provide emergency response support for actual and attempted attacks on the network and systems. |
| **Appointed Counsel** | Legal counsel appointed by Classic Tyler **(‘Appointed Counsel")** will be a member of the Response Team. The Appointed Counsel will be responsible for determining applicability of legal obligations in connection with the response, including notification obligations.The Appointed Counsel will also assist in drafting and coordinating communications to corporate executives, law enforcement, affected individuals, regulatory agencies, the general public and others if and as required or otherwise deemed appropriate (inconjunction with the President). The Appointed Counsel may also advise on any other matter as appropriate. |
| **President** | The Classic Tyler President is responsible for answering questions from the public (including the press), in consultation with the IT Director and Appointed Counsel. This includes coordinating with the Response Team to prepare any internal or external communications regarding the incident, serving as a subject matter expert regarding Classic Tyler’s desired tone and messaging, and responding to media inquiries, including preparing press statements if and as appropriate. When a Security Incident occurs, the President may disseminate information: if needed, to the public, after consultation with Appointed Counsel, the IT Director, and the CISO. |

**II. RESPONDING TO A SECURITY INCIDENT**

**10.0 Initial Reporting and Logging of Security Incidents**

All actual, potential, and suspected Security Incidents should be promptly reported to the Helpdesk by

phone or email. All employees and other authorized users should be trained to contact the Helpdesk when they

become aware of or suspect, a potential or actual Security Incident.

When a Security Incident is reported to the Helpdesk, the Helpdesk will promptly:

## Create and maintain current a Security Incident record

* Refer to the IT emergency contact list or affected department contact list and call the designated numbers in order on the list
* Contact the IT Director and the CISO; and
* Assist the IT Director and CISO with investigating the Security Incident and determining the appropriate

Incident Severity Classification, as defined in **Appendix B.**

Current contact information for the foregoing is:

## Helpdesk: email: help@myclassictoyota.com

* IT Director: David Hawkins Phone: (903) 330-3340; email: helpdesk@myclassictoyota.com

•· CISO: Amberlee Sipes Phone: (903) 530-4258 email: amberlee@myclassictoyota.com

At the time of the initial report, the Helpdesk will also log the following information:

## The name of the caller

1. Time of the call
2. Contact information about the caller
3. The nature of the incident
4. What equipment or persons were involved or effected

## Location of equipment or persons involved

1. How the incident was detected
2. When evidence was first noticed that supported the idea that the incident occurred

## Any supporting information such as screen shots or webpage URL' s



 **11.0 Incident Severity Classification**

The IT staff member or helpdesk member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. All staff members wi11 call those designated on the incident response list. The staff member will contact the incident response manager using both email and phone messages, while being sure other appropriate and backup personnel and designated managers are contacted. The staff member will log the information received in the same format as the Helpdesk team in the previous step. The staff member should also address the following if such information is available:

* 1. Is the equipment affected business critical?
	2. What is the severity of the potential. impact?
	3. Name of system being targeted, along with operating system, IP address and location.
	4. IP address and any information about the origin of the attack.
	5. Any screen shot or picture of the message.

Promptly after a Security Incident is reported, the IT Director (in consultation with the Helpdesk, the CISO, and any affected department should determine the appropriate Incident Severity Classification. Factors to be considered should include the elements listed in Appendix B, the nature and extent of the Security Incident, the type and sensitivity of the information involved, and the potential harm to Classic Tyler and to any other affected individual that has or may result from the Security Incident.

The Security Incident Severity Classification will dictate the appropriate response step (e.g. the proper communication strategy and the appropriate legal actions, if any).

* If the Incident Severity Classification is **Medium** or **High**, the Security Incident requires notification of the Response Team. In such case: the IT Director will initiate the Security Incident response processes and contact the Response Team.
* If the Incident Severity Classification is Low, the handling of the Security Incident should be directed to the appropriate department. For example, if the Security Incident involves one computer with an easily controlled virus, the IT Department should handle the response. However, the Helpdesk and IT Department should document the Security Incident and the response and submit a final report regarding the Security Incident including the initial record created by the Helpdesk, immediately after the Security Incident is resolved, to the IT Director.

Note that as the investigation of a Low level Security Incident progresses, the Security Incident should be reclassified if additional facts are discovered indicating that the Incident Severity Classification should be heightened, which could trigger the need to contact the Response Team.

**12.0 Activation of the Incident Response Team**

The Response Team is activated when a Security Incident has been classified as a Medium or High Security Incident, or at the request of the IT Director. Once the Response Team has been activated it will promptly convene in person or via teleconference to assess the conditions of the Security Incident, begin recording all the relevant facts, and begin the response process.

# 13.0 Procedures to Guide Response Team in Responding to Potential Security Incidents

The Response Team shall take the following steps in response to any potential Security Incident

# 13.l Initial Response

Once the Response Team has been assembled and made aware of the suspected Security Incident, it must take immediate steps to assess the circumstances and details surrounding the Incident, including the nature and scope of the unauthorized access and information affected. This includes verifying that aSecurity Incident has actually occurred and identifying (i) what Information Assets are affected, (ii) which users are involved, and (iii) the potential business impacts. The Response Team should verify enough information about the Incident so that an overall response strategy can be formulated.

The Response Team must also determine the most appropriate response strategy, given the circumstances of the Incident. The strategy should take into consideration technical, business, and legal factors. Because the response strategy can have repercussions that influence employees, shareholders, and consumer confidence, it should be approved by senior management.

Factors that should be considered in deciding how to respond to the Security Incident include the following:

* + When the Security Incident occurred and when it was discovered
	+ How critical. the affected systems are·
	+ The sensitivity of the compromised or stolen information
* who the potential perpetrators are
* whether or not the Incident is known to the public or should or must be disclosed to the public or other- third parties
* The level of unauthorized access attained by the perpetrator
* The apparent skill of the perpetrator
* How much system and user down time can be tolerated
* The overall dollar loss involved and
* Potential legal obligations.

# 13.2 Investigate the Scope of the Incident, including the Information Affected

The investigation phase determines the who, what, when, where, and how surrounding the Security Incident. After determining Classic Tyler’s approach in responding to the Security Incident, the Response Team should begin its investigation and assign resources (personnel and financial) to the response and recovery effort at a level appropriate for the severity of the Security Incident.

In conjunction with its investigation, the Response Team must gather and preserve evidence regarding the Security Incident, such as audit trails, logfiles, contents of files, key pass records, sign-in sheets, records from surveillance equipment etc. No information should be deleted or destroyed.

The evidence gathering must be performed in a forensically sound manner. This is especially important if it is necessary that the evidence will later be admissible in court. Where appropriate, the Response Team should also consider the use of specialized technical assistance and advice from a third party expert to ensure the evidence is gathered in a forensically sound manner. *See Section 15.0 below.* Nevertheless, the physical security of individuals should always be the first priority. · ·

Once evidence has been gathered, the evidence must be analyzed to determine the cause of the Security Incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the incident, and so forth. An assessment must also be made to determine how far the Security Incident has spread, e.g., which systems are involved and the extent to which they were compromised.

Once the evidence is gathered, protecting the evidence is essential. Evidence can be easily contaminated either accidentally or intentionally.

The investigation should focus on determining:

* The nature and scope of the incident,
* The types of Protected Information or other Information Assets that may have been accessed or misused and the format the Protected Information was in when it was accessed
* Whether personal information triggering breach notification requirements has been subjected to unauthorized access or acquisition, and if so, the number of affected individuals by state of residence.

### Contain and Eradicate the Incident

If the incident is on-going, IT Director, the CISOand Appointed Counsel shall determine whether steps should be taken by the IT Director to immediately contain the incident, and whether outside forensic investigators should be immediately consulted. Appropriate steps to contain the Security Incident, include:

* Identify the source of the Security Incident
* Determine the full extent of the Security Incident
* Identify and isolate the compromised system from the network
* Implement stopgap measures to eliminate any active threats; and
* Update security and Security Incident report documentation with eradication information.

### Evidence Preservation

The Response Team shall immediately preserve evidence, including suspension of any destruction and

overwriting of logs. The IT Director shall be responsible for the establishment and maintenance of the chain of custody of relevant data and equipment. Appointed Counsel will advise the IT Director regarding whether and when the IT Director should instruct all employees to preserve all communications relating to the incident.

### Recoverv Procedures

The Response Team must take appropriate steps to ensure an efficient recovery from the Security Incident. Once the Security Incident is contained and eradicated, the Response Team must assist in restoring the systems and Information Assets to normal operation. This may require reloading data from backup tapes, reinstalling systems from their original distribution media, etc.

Once the affected Information Assets have been restored, they should be tested to make sure they are no longer

vu1nerab1e to the type of attack or problem that caused the Security Incident. Computer systems shou1d also be tested to ensure they will function correctly when placed back into production or on the network.

If possible, the recovery procedures should include reversing any damages caused by the Security Incident. This will help to minimize the costs, both tangible and intangible, associated with the Security Incident. However, care must be taken to ensure that no relevant evidence is destroyed in the process.

* 1. **Document the Incident and Classic Tyler’ Response**

Throughout the response process, the IT Director shall maintain appropriate documentation of the incident, Classic-Tyler’ response thereto, and any communications with regulators, law enforcement, affected individuals and others. Such documentation should include the following:

* + 1. How the incident was discovered
		2. The category of the incident

(3) How the incident occurred, whether through email, firewall, etc.

1. Where, the attack came from, such as IP addresses and other related information about the attacker
2. What the response plan was
3. What was done in response
4. Whether the response was effective

14**.0 Third Party Forensic Investigations**

Depending on the nature of the Security Incident and corresponding criticality, the Response Team may decide to perform a forensic investigation. This may be appropriate, for example, in the case of incidents that appear to require investigation to determine the scope of the incident and information exposed, and to ensure that the incident is promptly contained. A forensic investigation will allow Classic-Tyler to gain a better understanding of the intrusion and the attacker. A forensic investigation may be performed by a third-party forensic analyst

with the appropriate certifications and in a manner that is consistent with industry standards. A forensic expert should also be used when there is a need to extract information from the compromised system(s) without altering the original data, and when it is necessary to ensure the admissibility of evidence. In

order to interpret the degree to which malicious activity has occurred and to understand the extent of the

incurred damage, the forensic investigation is dependent upon the preservation of the information.

If forensic investigators are deemed appropriate, Appointed Counsel shall engage the forensic investigators on behalf of Classic Tyler pursuant to a claim of attorney-client privilege, unless Appointed Counsel recommends, or the Response Team otherwise decides, that they prefer not to engage the forensics investigation pursuant to attorney-client privilege due to the circumstances surrounding the incident.

# 15.0 Contacting Law Enforcement

The Response Team, with the assistance of Appointed Counsel, must determine whether contacting law enforcement is required by law and/or desirable. Law enforcement should generally be contacted when the Security Incident is the result of criminal activity. Contacting law enforcement may also be required under certain other circumstances. The Appointed Counsel should advise the Response Team when these types of Security Incidents occur and assist in any such notification.

# Contacting Insurance Broker

The CISO shall contact Classic Tyler’s insurance broker in order to determine availability of coverage for costs associated with responding to the Incident. If coverage is available, the CISO shall confirm with the broker any specifics of the coverage, including issues such as:

* + - whether specific vendors must be used
		- whether prior insurer consent to retention of vendors/incurring of expenses is required
		- the amount of any deductibles/self-insured retentions and limits of coverage
		- requirements to notify the insurer of the incident/claim.

## **17.0 Notifications and Communications Regarding the Security Incident**

Determining whether and how to communicate information regarding the Security Incident to management,

employees and externally is a very important step in the Incident response process. Following a Security Incident, it will also be necessary to determine whether Classic Tyler is required by law, industry regulations or public relations purposes to notify third parties about the Security Incident. This might include notification to individuals whose information was, or potentially was compromised or affected by the Security Incident, as well as regulators, enforcement agencies, and others. There may also be reasons to notify business partners and the media.


## **17.1 Notices Required bv Law or Contract**

In consultation with the Response Team, Appointed Counsel shall review the details of the Security Incident and applicable legal and contractual requirements to determine whether any legal obligations require notice to any of the following individuals or entities, and if so, the requirements for such notices:

* Law enforcement
* Affected individuals
* Government regulators
* Consumer reporting agencies, the press, and others and

•· Contractual counterparties

In the case of notices required by law or contract, Appointed Counsel will either draft such notices in coordination with the Response Team or review such notices for compliance with applicable law before they are sent out.

# 17.2 Coordination of Communications and Notices

Communications of any legally required notices, as well as all other communications (e.g. to employees, the press, and others) should be coordinated by the President with the advice and assistance of Appointed Counsel. The IT Director and President shall also determine whether to engage a PR/Media Relations firm to assist with press issues and other inquiries, and to advise on customer relations and public relations issues.

Before providing any notification or public statement, the following should be considered:

* Who will be contacted
* How information will be communicated
* When news will be released

## Who will be told

* What information will be released and what will be withheld
* Requirements of the applicable breach notification statutes and regulations (state requirements are summarized in **Appendix C)** and
* The desired press strategy in connection with any notifications and in the event of media attention prior

to issuance of notice.

# 18.0 Follow-Up and Maintenance

1. **Security Incident Review and Follow-Up**

Within 30 days following conclusion of the Incident response, and again as necessary or appropriate, the Response Team shall meet to discuss lessons learned, and improvements that can be implemented to improve Classic Tyler Motors’ response to, and help to prevent occurrence of, future Security Incidents. The IT Director shall prepare an Incident Review Report summarizing such discussions, conclusion, and steps to be taken, and update Classic-Tyler Motors' policies and procedures, including this Response Plan, and implement other changes deemed appropriate.

The Questions to Guide Post-Breach Discussion and Incident Review Report attached as **Appendix D** shall guide such discussions and be completed by the IT Director to reflect such discussions.

# .Regular Incident Response Plan Review and Update

At a minimum, this Incident Response Plan must be reviewed and updated as appropriate on an annual basis and following all High severity Security Incidents.

Such review should examine the entire Incident Response Plan. In addition, new federal, state and industry requirements should be considered and, if necessary, reflected in revisions to the Incident Response Plan.

1. **Employee Awareness and Education**

Employee awareness is critical for the success of the Incident Response Plan. Classic-Tyler Motors will endeavor to train all employees regarding their obligations under the Incident Response Plan. The Response Team will collaborate on the design, coordination, and implementation of such training procedures.