Information Security Management
Policy Document

Information Security Policy

Version 3.0
<December 21, 2016>

History Log Date		
Version	**Date**	**Author**
Version 3.0	July 2016	TREC Pacific Corporation
Version 3.0	December 21,2016	TREC Pacific Corporation

1. Introduction

This policy document provides the framework to develop and disseminate an information security policy in order to achieve PCI compliance. This policy document is the master document, which is supported by other documents governing PCI compliance within TREC Pacific Corporation

2. Information Security Policy Coverage

Information Security Policy of the organization encompasses:

- Information Security Policy (this document)
- Access Control Policy
- Data Encryption Policy
- Data Retention, Retrieval and Secure Disposal Policy
- Human Resource Policy
- Change Management Policy
- Password management policy
- Network Security Policy
- Data Encryption & Key Management Policy
- Audit Log and Monitoring Policy
- Patch Management Policy
- Malicious Code Policy
- Software Development Policy
- Vulnerability Management Policy
- Physical Access Control Policy
- Remote Access Policy
- Risk Assessment Methodology
- Third Party Management policy

3. Policy Dissemination **(PCI DSS 3.0 Reference – Requirement 12.1)**

The information security policy must be published and disseminated to all relevant system users (including vendors, contractors, and business partners).

4. Risk Assessment PCI DSS 3.0 Reference – Requirement 12.2.a

The organization shall carry out an annual risk assessment process that would identify major strategic developments in the industry, emerging threats, & vulnerabilities, to business and IT assets of the company and report results in a formal risk assessment document.

Standard Risk assessment methodologies can be considered which includes but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.

5. Information Security Policy Review

The information security policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. **PCI DSS 3.0 Reference– Requirement 12.1.1**

6. Information Security Policy Responsibilities

The information security policy will define the person(s) responsible for implementing and maintaining information security throughout the organization.

- Establish, document, and distribute security policies and procedures.
- Monitor and analyze security alerts and information, and distribute to appropriate personnel.
- Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

Area Responsible :
Manager :
Information Security team :

7. Formal Security Awareness Program

- ✓ Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.
- ✓ Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions).

8. Formal Acknowledgment Information Security Policies

The organization should require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

9. Employee Screening and Background Checks

The current employees and the potential employees in the company would be screened through a defined procedure to minimize the risk of attacks from internal sources.

10. Third Party Service Provider Contractual Requirements

If cardholder data is shared with service providers, then contractually the following is required:

a) Service providers must adhere to the TREC Pacific Corporation's compliance requirements.
b) Agreement that includes an acknowledgment that the service provider is responsible for the security of cardholder data the provider possesses.

11. Connected Entity Requirements

All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

a) Maintain list of connected entities
b) Ensure proper due diligence is conducted prior to connecting an entity.
c) Ensure the entity is PCI DSS compliant.

d) Connect and disconnect entities by following an established process.

12. Asset Classification

Data and information classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored or transmitted. The classification of the data should determine the extent to which the data needs to be controlled/secured and is also indicative of its value in terms of Business Assets.

The term Business Assets, for the purpose of the scope of this policy, refers to any information upon which the organization places a measurable value. By implication, the information is NOT in the public domain and would result in loss, damage or even business collapse, was the information to be lost, stolen, corrupted or in any way compromised.

Proper access controls and privilege levels are to be set before accessing sensitive cardholder data by any user internally. Media containing sensitive data shall only be distributed to the authorized in-house employees.

All applications and network hardware equipment which are accessible to the external parties and which transmit or deal with sensitive cardholder data should be protected by strong access control and authentication mechanisms.

Media containing sensitive data must not be handed over to any external entity or third party unless until authorized by the management with proper business justification.

The following procedure should be followed for the purpose of data classification:

Computer output, regardless of media, which is classified in accordance with this classification scheme will be marked on the top and bottom of each page and/or on each output screen with the appropriate classification, except for the General classification, when it is created by the system.

1.1 General

This classification includes all information that may normally be considered as General information, however, for business reasons management has determined that its use and dissemination needs to be controlled.

Shredding of this information is not required for disposal.

1.2 Proprietary

All data and information, except for media releases approved by management, used in conducting day-to-day business is regarded as proprietary and is not intended for discussion or disclosure to other than <Name of the Organization> staff.

Shredding of this information for disposal is desired but not required.

1.3 Restricted

Some of the data and information retained in the automated systems and on other media (e.g. microfiche, microfilm, and paper files) is critical to the continued profitability of the organization. Other data and information is regarded as personal since it pertains to our employees. To provide adequate protection for this type of material it will be given a classification level of Restricted for identification.

Shredding of this information for disposal is required.

1.4 Confidential

This category of information includes company plans, the premature release of which could be detrimental to the company's strategic plan (e.g. acquisitions being planned/negotiated) or which could result in the filing of civil or other litigation (e.g. release of additional stock for sale or a company buy back of outstanding stock). Also included in this category is any other information specifically designated as Secret by Senior Management.

This information is not authorized to be stored on any computer system except for desktop or laptop systems. When stored on desktop or laptop systems the information will be encrypted, using approved encryption software, to provide adequate protection. Additionally, this information will not be transmitted over any computer network within or between <Name of the Organization> facilities unless it is encrypted, using approved encryption software.

If this information is stored on removable storage media, then such items should be properly identified and stored in a locked desk drawer, cabinet or safe when not in use.

Shredding of this information for disposal is required.

Guidelines for data classification and sensitivity must be documented and communicated to responsible data/information owners and all support responsible in order that information receives an appropriate level of protection.

13. Roles and Responsibilities PCI DSS 3.0 Reference – Requirement 12.5

13.1 Chief Security Officer (or equivalent)

Responsible for overseeing all aspects of information security, including but not limited to:

- ✓ Creating and distributing security policies and procedures
- ✓ Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
- ✓ Creating and distributing security incident response and escalation procedures that include:
  - Roles, responsibilities, and communication
  - Coverage and responses for all critical system components
  - Notification, at a minimum, of credit card associations and acquirers
  - Strategy for business continuity post compromise
  - Reference or inclusion of incident response procedures from card associations
  - Analysis of legal requirements for reporting compromises (for example, per California bill 1386)
- ✓ Annual testing
- ✓ Designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
- ✓ Plans for periodic training
- ✓ A process for evolving the incident response plan according to lessons learned and in response to industry developments

- ✓ Maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)
- ✓ Review security logs at least daily and follow-up on exceptions

13.2 The Information Technology Office (or equivalent)

Shall maintain daily administrative and technical operational security procedures that are consistent with the organization's compliance requirements that include:

- ✓ User account maintenance procedures
- ✓ Log review procedures

13.3 System and Application Administrators

- ✓ Monitor and analyze security alerts and information and distribute to appropriate personnel
- ✓ Administer user accounts and manage authentication
- ✓ Monitor and control all access to data
- ✓ Maintain a list of connected entities
- ✓ Perform due diligence prior to connecting an entity, with supporting documentation
- ✓ Verify that the entity is compliant with relevant compliance standards, with supporting documentation
- ✓ Establish a documented procedure for connecting and disconnecting entities
- ✓ Retain audit logs for at least one year

13.4 The Human Resources Office (or equivalent)

Responsible for tracking employee participation in the security awareness program, including:

- ✓ Facilitating participation upon hire and at least annually
- ✓ Ensuring that employees acknowledge in writing that they have read and understand the company's information security policy
- ✓ Screen potential employees to minimize the risk of attacks from internal sources

13.5 Internal Audit (or equivalent)

Shall be responsible for executing a risk assessment process that identifies threats, vulnerabilities and results in a formal risk assessment.

13.6 Contracts manager (or equivalent)

Ensure that for service providers with whom cardholder information is shared:

- ✓ Contracts require adherence to TREC Pacific Corporation by the service provider
- ✓ Contracts include acknowledgment or responsibility for the security of cardholder data by the service provider

14. User Access

14.1 Responsibilities

The IT Department is responsible for creating, documenting and maintaining individual user/user group profiles that meet the requirements of Access Control Policy

14.2 Classification of users

Users are also classified in terms of:

- Least privileges that are necessary to perform the job responsibilities
- Individual personnel's job classification and function

14.3 Privileges

Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated from the user concerned to the IT Department which reviews the reasons why the privilege is required and the length of time for which it is required.

15. User registration and de-registration (Creation & Deletion)

User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access. Every user's proposed access rights

are documented in a user form, which details the systems/services/applications/information assets to which access is to be granted, together with the level of access that is granted, taking into account the ***Access Control Policy***. If a user is to be granted access rights other than the standard ones set out in ***Access Control Policy,***then the specific additional authorization of the Management is also required.

- The System Administrators authorizes access to the system/asset and passes the User Creation/Deletion form to the Technical Support and the user name/ user ID is created/deleted and administered.

- The IT Department maintains a list of authorized Users, Administers changes in access rights and removes users.

- The disciplinary policy will be invoked in cases of attempted unauthorized access.

16. Password Management

The minimum password management requirements for the systems are as follows:

Requirement	**Condition**
Users to be issued with a temporary password, and to be forced to change on first log in	○ Should be mandatory for Application Access for Individual Users – Internal and External
Password Expiry	○ Minimum of 90 days
Password length	○ Minimum of 7
Password complexity	○ Should be high and should contain at least one alphabet and one numeric character
Password history	○ Last 4 passwords
Period of Inactivity	○ Maximum of 90 days
Storage	○ Encrypted
Number of failed attempts for lockout	○ Maximum of 3
Lockout period	○ At least 30 minutes

Session Timeout	○ Maximum of 15 minutes of inactivity

- First-time passwords for new users are set to a unique value for each user and MUST be changed after first use.

- The default passwords on all new equipment are changed to conform with TREC Pacific Corporation Password Policy requirements before the equipment is brought into Production.

17. User Authentication

Users are authenticated at log-on by providing both their user name and their password within the parameters of the log-on system as per the section 6 of this document.

18. Review of access rights

- Access rights are reviewed by Information Security Team quarterly and their adequacy is confirmed.

- User access rights are reviewed when a user's role or location within organization changes in any way

19. Customer cardholder data Security

PCI DSS 3.0 Reference – Requirement 12.9

(Please ensure that you acknowledge in written agreement with customer confirming the customer’s cardholder data in accordance with all applicable PCI requirements).

TREC Pacific Corporation shall acknowledge in writing to all customers that the TREC Pacific Corporation will maintain all applicable PCI DSS requirements to the extent that TREC Pacific Corporation handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.

Information Security Management
Policy Document

TREC Pacific Corporation is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy was approved by the Security Information Officer and is issued on a version controlled basis under his/her signature