INTRODUCTION AND SCOPE

Introduction

This document explains READYCALL CENTER Corporation's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. READYCALL CENTER Corporation management is committed to these security policies to protect information utilized by READYCALL CENTER Corporation in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, READYCALL CENTER cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, ver. 3.0,. Should READYCALL CENTER Corporation implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of READYCALL CENTER Corporation to determine the appropriate compliance criteria and implement additional policies and controls as needed.

INFORMATION SECURITY POLICY

ReadyCall Center as being service provider for TracFone wireless, must be aware of all needs from the customer perspective, comply with proper asset use, in case of any security gap, inform accordingly.

Any process performed by specific credentials will be solely and only responsibility of the username, if by any reason you suspect your account as been compromised, follows chapter 12 guidelines.

Dormant accounts will be disabled.

Password complexity includes one special character, one uppercase letter, at least 8 characters, and it cannot contain your name.

All usernames created By ReadyCall are confidential and must be delivered to uts final user by authorized parties, requesting password change as initial process.

Remaining accesses granted by TracFone are governed by TracFone's business needs

Please change your password as soon as is requested.

Policy review and evaluation

In accordance to the PCI needs PCI-DSS V3.2 Requirement 12.1.3 the policies and rules have to be reviewed at least annually. The purpose of the review is to ensure that the policies and procedures are up-to-date with the newest updates tools and requirements new potential threats, exploits and other changes that can affect the information security at the Call Center. This policy can be changed and amended as required.

Exceptions

In some occasions our customer TracFone might require immediate actions processes and requirements that have must override some policies, however the exception has to be documented, and the areas where a possible override is included in the policies.

If the requirement represents a potential harm to the center, ReadyCall can advise TracFone about it, but follow the rules.

Disciplinary actions

All the processes rules and policies applied are indivisible rules and avoiding any part of the document by any ReadyCall employee, the processes can include immediate termination, and civil consequences if the personnel is involved on data leaks on purpose.

Usage of the devices

All devices including PC's and devices should be used only for business purpose only. Personal use is extremely forbidden as well as the usage of removable mass storage devices.

Users must not exploit vulnerabilities or deficiencies systems security to damage systems or information, to obtain resources beyond those they have been authorized to obtain, to take resources away from other users, or to gain access to other systems for which proper authorization has not been granted. Users must report any weaknesses in computer security and any incidents of possible misuse or violation of this agreement to IT Operations.

Privacy

ReadyCall owns the information and processes created by it's staff teams to satisfy our customer needs. With the exception of customer information, and tools that belongs to TracFone Wireless INC. ReadyCall may log, review, and otherwise utilize any information stored on or passing through its Computing Resources. For these same purposes, ReadyCall may also capture the use of the resources such as telephone numbers dialed websites visited. ReadyCall reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of websites visited, and other information stored on or passing through the network computersThis in order to guarantee the compliance of the policies and rules.

All the information should and has to remain inside ReadyCall unless explicit permission, no information can be reviewed by third parties teams unless they have an appropriate permission.

This also includes

- Physical Controlled areas.
- Logical restrictions to tools and information data storage.
- Logical protection devices policies and accesses combined to have a secure environment i.e. passwords firewalls, web filter Content Manager. Please review configuration and documentation on the IT Chapter 1,2
- Investigative personal information is being inappropriately collected, used or disclosed. Chapter 10 PCI Compliant Agent Tracking.

Email Usage.-

When justified by business needs it has to be requested either by operations manager or Call Center director, for processing after validating business needs.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider.(PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.5)
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering. (PCI Requirement 1.3.6)

No mobile devices are to be broughtinside opertations or connected to the Networkr

Clean Policy is a MUST comply therefore no pen, paper mass media or electronic devices inside operations

. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. READYCALL CENTER Corporation must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (PCI Requirement 2.2)

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

System administrators are responsible to insure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.5)

System Configuration standards must address new vulnerabilities as they arise updating requirements and preventive measures (PCI Requirement 2.2.b)

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

- Although we Don't store or Process CHD, we have to be sure to protect it by not placing this information anywhere, and by no mean any confidential information incluing CVV,SSN,Credit card or PAN can be transmitted outside any tool that belongs to our customer. Which executes all process over secure protocols

Requierment 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

Use ONLY DS DPPORTAl, do not attemnt to exploit vulnerabilities

Requirement 5: use and Regularly Update Anti-Virus Software or Programs

Anti-Virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, READYCALL CENTER Corporation will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

Requirement 6: Develop and Maintain Secure Systems and Applications

Risk and Vulnerability

READYCALL CENTER Corporation will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to READYCALL CENTER cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)

Privileges must be assigned to individuals based on job classification and function (as is described on the access matrix). (PCI Requirement 7.1.3)

It is your Duty to inform if additional accesses are granted on your account to your superior or IT department. (PCI Requirement 7.1.3)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Remote Access

Renore access is explicitly forbidden and shall be penalized if attemptred. (PCI Requirement 8.3)

Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure All Areas and Media Containing Cardholder Data

Operations floor is like a banck where clean desk policy and no electronic devices are allowed.

Destruction of Data

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Do Not attempt to store CHD on your system

Requirement 10: Regularly Monitor and Test Networks

Audit Log Collection

READYCALL CENTER Corporation will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges. (PCI Requirement 10.2.2)
- All invalid logical access attempts (failed logins). (PCI Requirement 10.2.4)
- Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

READYCALL CENTER log generating and collecting solution will capture the following data elements for the above events:

- User identification. (PCI Requirement 10.3.1)
- Type of event. (PCI Requirement 10.3.2)
- Date and time. (PCI Requirement 10.3.3)
- Success or failure indication. (PCI Requirement 10.3.4)
- Origination of event. (PCI Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

Audit Log Review

READYCALL CENTER systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.

- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

READYCALL CENTER Corporation must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). (PCI Requirement 10.7)

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, READYCALL CENTER Corporation will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).
- Wireless devices attached to a network port or network device.

To facilitate the detection process, READYCALL CENTER Corporation will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10). (PCI Requirement 11.1.2)

Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), READYCALL CENTER Corporation will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all "high" vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.2)

For both internal and external vulnerability scans, READYCALL CENTER Corporation shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. (PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, READYCALL CENTER Corporation must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

Review and consideration of threats and vulnerabilities experienced in the last 12 months.

Retention of penetration testing results and remediation activities results.

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

READYCALL CENTER Corporation shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1)

Critical Technologies

READYCALL CENTER Corporation shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Authentication for use of the technology. (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access. (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies. (PCI Requirement 12.3.6)

- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

Security Responsibilities

READYCALL CENTER policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

The IT Manager shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

Reporting an Incident

The IT department should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the IT Manager to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the IT Manager/ Call center Director about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the IT Department

Document any information you know while waiting for the IT Departmnet to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response Policy (PCI requirement 12.10.1)

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis.

All notifications MUST BE ISSUED BY TRACFONE, however in lieu of policy here's the process

1. Notify applicable card associations.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by

the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

Discover Card

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state From where TracFone will address with Credit Card Brands.
4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the IT Manager will work with legal Client.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the IT Security department and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

READYCALL CENTER Corporation shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Including and not limited to password handling, surrender,

Service Providers

READYCALL CENTER Corporation shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- Maintain a list of service providers. (PCI requirement 12.8.1)

- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. (PCI requirement 12.8.2)
- Implement a process to perform proper due diligence prior to engaging a service provider. (PCI requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status. (PCI requirement 12.8.4)
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI requirement 12.8.5)