Internet Privacy Policy

[Last updated 05/01/2013]

To underscore our commitment to privacy and our vision that good privacy is good business, we have adopted this Internet Privacy Policy for www.townofparadise.com and aca.townofparadise.com which are operated by Town of Paradise ("Town"), 5555 Skyway, Paradise, CA 95969. This site is not directed at children under the age of 13.

INFORMATION COLLECTION

I. Personally-Identifiable Information

This site only collects personally identifiable information ("PII") from you if you choose to provide this information to us. Personally identifiable information collected with your consent may include, for example, name, mailing and credit card billing address(es), telephone number, e-mail address, or other vital event, credit card number, demographic information which may be associated with any response you provide to survey questions, information relating to any orders you place, or any inquires you may make through our web site. We do not share, sell, rent or trade PII with third parties except where is required in the normal order of business such as processing of credit card information relating to a payment.

II. Cookies

“Cookies” are small pieces of information that are stored by your browser on your computer's hard drive. This site uses cookies to determine whether a visitor is unique or whether the visitor has viewed our site before. Our purchase process also uses cookies. This information allows us to recognize you as a customer, along with your account information. Very simply, this useful tool keeps you, our customer, from having to retype information that you've already entered. While most browsers are set to accept cookies by default, you can set yours to refuse cookies or to alert you before accepting them. Your browser manufacturer has information on changing the default setting for your specific browser. Failure to accept cookies may limit your ability to place orders through our website. We do not link the information we store in cookies to any PII you submit while on our site.

III. Nonpersonally-identifiable information

This site also collects nonpersonally-identifiable information. For example, as you browse this web site we may collect information about your visit, but not about you personally. Via Web server logs, for example, we may monitor statistics such as: the number of people that visit our site, which page(s) are visited on our site, from which domain our visitors come (e.g., aol.com, hotmail.com, etc.), and which browsers people use to visit our site (e.g., Apple Safari, Microsoft Internet Explorer, Google Chrome, etc.). Our web site uses outsourcing programs to assist us in analyzing this data to better tailor our web site.

INFORMATION USE AND CONSUMER CHOICE

The information collected by this web site is used only for responding to your inquiries and otherwise corresponding with you, for processing transactions you request, maintaining your account, (if you have one), and for the administration, review and/or the improvement the content of our web sites. We do not share, sell, rent or trade PII with third parties for their promotional purposes.

We may contact you in response to your comments or inquiries, as part of the maintenance of your account or on-line request or in order to complete a transaction that you requested.

If you decide that you do not want to receive further e-mails regarding your business with the Town, you can reply to the e-mail.

ONWARD TRANSFER

We may disclose information you provide to us to third parties (such as credit card processors) in order to complete a transaction that you requested. If, for example, you pay for a transaction using a credit card, disclosing that information for processing purposes is necessary to complete the transaction. In other cases, it may be necessary to disclose information you provide about yourself or third parties (government agencies) in order to complete your request.

We may also outsource some tasks, including the operation of some website functions that require access to information you supply online. In such cases, however, we require that the companies acting on our behalf abide by our privacy policy and institute safeguards to protect the confidentiality of your information.

Finally, please note that we may disclose personal information when required by law or in the good faith belief that such action is necessary in order to conform with the law or to comply with a legal process.

ACCESS AND CORRECTION

We strive to maintain the accuracy of the information collected through this Web site. Upon proper identification, we will provide you (whether you are a consumer or a customer) with access to personally-identifiable information you provide through this Web site for as long as we maintain that information in a readily accessible format. Similarly, we permit and encourage you to correct inaccuracies in the information you submit to us through this Web site. Please note, however, that correction of information is not always possible.

If you wish to access information that you have submitted through this web site or to request the correction of any inaccurate information you have submitted through this site, please use the mechanisms provided by the site or send an e-mail to customersupport@townofparadise.com.

SECURITY

We take steps to protect against the loss, misuse, or unauthorized alteration of PII collected through this web site. We recognize the importance of security for all PII collected by our web site. We exercise care in providing secure transmission of your information from your PC to our servers.

Once we receive PII, we take steps to protect its security on our systems. In the event we request or transmit sensitive information, such as credit card information, we use industry standard, secure socket layer (“SSL”) encryption.

OTHER WEB SITES

This Internet Privacy Policy only applies to the web site(s) identified in the first paragraph of this Privacy Policy. Our web site, however, may include links to other web sites which may be operated by third parties. If you visit a web site not listed above, we recommend that you review the Internet Privacy Policy of that web site to determine how the operator of that web site will handle personal information collected through that web site.

POLICY CHANGES

We may revise this Internet Privacy Policy from time to time. If the Town makes any material changes to this Internet Privacy Policy, the date of the most recent revision will be indicated above so that you can determine whether there

have been any material revisions since your last visit. If we are going to use your PII in a manner different from that stated at the time of collection we will notify you via email. You will have a choice as to whether or not we use your information in this different manner.

If you have questions or concerns regarding this Internet Privacy Policy, please contact us at:

Town of Paradise
5555 Skyway
Paradise, CA 95969

Telephone: 530-872-6291
E-mail: customersupport@townofparadise.com

Internet Refund Policy

[Last updated 05/01/2013]

To underscore our commitment to privacy and our vision that good privacy is good business, we have adopted this Internet Refund Policy for www.townofparadise.com and aca.townofparadise.com which are operated by Town of Paradise ("Town"), 5555 Skyway, Paradise, CA 95969. This site is not directed at children under the age of 13.

REFUND INFORMATION

Users agree to comply with the stated policies and procedures of the site. If all charges, fines, and/or fees have been paid and as a result you have a credit balance, a refund equal to that amount will be refunded. In all other cases, refunds are determined on a case by case basis unless otherwise addressed in the rules and regulations, charter, or ordinances of the Town.

Any refund of payments originally made by credit card shall be credited using the same credit card.

REQUESTING A REFUND

If you would like to request a refund, please contact us at:

Town of Paradise
5555 Skyway
Paradise, CA 95969

Telephone: 530-872-6291
E-mail: customersupport@townofparadise.com

POLICY CHANGES

We may revise this Internet Refund Policy from time to time. If the Town makes any material changes to this Internet Refund Policy, the date of the most recent revision will be indicated above so that you can determine whether there have been any material revisions since your last visit.

If you have questions or concerns regarding this Internet Refund Policy, please contact us at:

Town of Paradise
5555 Skyway
Paradise, CA 95969

Telephone: 530-872-6291
E-mail: customersupport@townofparadise.com

Credit Card Security Policy

[Last updated 05/22/2013]

This document explains the Town of Paradise's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. The Town of Paradise is committed to these security policies to protect information utilized by the Town of Paradise in attaining its business goals. All Users 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, the Town of Paradise cardholder environment consists only of an application 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. 2.0, October, 2010.

Requirements:

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 Town of Paradise, and/or which is out of the Town's ability to control or manage. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted 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)

All open ports and services must be documented. Documentation should include the port or service, source and destination, and a business justification for opening said port or service. (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 (PCI Requirement 1.3.5)
- Firewalls must implement stateful inspection, also known as dynamic packet filtering (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers must not have access to the cardholder data environment. (PCI Requirement 1.4)

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:

- 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 for authentication and transmission of data over wireless networks. (PCI Requirement 2.1.1)

Unneeded Services and Protocols

Only necessary services, protocols, daemons, etc., as needed for the function of the system may be enabled. All services and protocols not directly needed to perform the device's specified function must be disabled. (PCI Requirement 2.2.2)

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

3. Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

The Town of Paradise will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

4. Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). Only trusted keys and/or certificates can be accepted. For SSL/TLS implementations HTTPS must appear as part of the URL, and cardholder data may only be entered when HTTPS appears in the URL. (PCI Requirement 4.1)

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

5. Use and Regularly Update Anti-Virus Software or Programs

Anti-Virus

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)

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

6. Develop and Maintain Secure Systems and Applications

Security Patches

All critical security patches must be installed within one month of release. This includes relevant patches for operating systems and all installed applications. (PCI Requirement 6.1)

7. Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to Town of Paradise's 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 7.1.1)
- Privileges must be assigned to individuals based on job classification and function (also called "role-based access control). (PCI Requirement 7.1.2)

8. Assign a Unique ID to Each Person with Computer Access

Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (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 8.5.6)

9. Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.6)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.7.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.7.2)

Logs must be maintained to track all media that is moved from a secured area, and appropriate approval must be obtained prior to moving the media. (PCI Requirement 9.8)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.9)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Container stored information waiting to be destroyed must be secured to prevent access to the contents. (PCI requirement 9.10.1)

10. Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, Town of Paradise will perform testing to ensure there are no unauthorized wireless access points present in the cardholder environment. (PCI Requirement 11.1)

This testing must detect and identify any unauthorized wireless access points, including at least the following:

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

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.) it must be configured to generate alerts

Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.9).

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), the Town of Paradise will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be repeated until passing results are obtained, or until all “high” vulnerabilities as defined in PCI Requirement 6.2 are resolved. (PCI Requirement 11.2.1, 11.2.3)

Quarterly 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). (PCI Requirement 11.2.2, 11.2.3)

11. Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

The Town of Paradise 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 12.1.3)

Critical Technologies

The Town of Paradise 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 de-activation after use (PCI Requirement 12.3.9)

Security Responsibilities

The Town of Paradise's 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 Manager should be notified immediately of any suspected or real security incidents involving cardholder data:

- Contact the IT Manager via email **and** phone to report any suspected or actual incidents.
- No one should communicate with anyone outside of their supervisor(s), Town Manager, or the IT Manager about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Town Manager.

- Document any information you know while waiting for the Town Manager or IT Manager 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

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

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 where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm

4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the IT Manager will work with the Town Attorney and the Town Manager to identify appropriate forensic specialists.

5. Eliminate the intruder's means of access and any related vulnerabilities.

6. Research potential risks related to or damage caused by the intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, the Town Manager, IT Manager, and all other 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

The Town of Paradise 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)

Service Providers

The Town of Paradise 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)