Granite City Food & Brewery/ Cadillac Ranch

Security Awareness Guide

Version 1.02

REVISED 11/11/2015

GRANITE CITY food & brewery

Cadillac Ranch
THE GREAT ALL-AMERICAN BAR & GRILL

Company policy & procedure on ensuring cardholder information security

TABLE OF CONTENTS

PURPOSE OF THE SECURITY AWARENESS GUIDE

This document is established to educate employees of the importance of securing cardholder information. It contains the minimum training for users on the network to create awareness of basic computer threats to protect themselves, Granite City Food and Brewery and Cadillac Ranch Brand, the Enterprise Network, Cardholder Data and Sensitive Authentication Data. The policies outlined throughout this guide apply to all employees with access to sensitive or regulated data.

The following items will be reviewed during new hire orientation and at a minimum on an annual basis. Details of each are provided in the sections that follow.

- ☑ Basic Cardholder Data Security Information
- ☑ Approved Crash Kit Process
- ☑ Security Fraud Awareness
- ☑ Incident Response Policy and Plan
- ☑ Facility Access Control Policy
- ☑ Acceptable Use Policy

1. Basic Cardholder Data Security Information

1.1 WHY PCI DSS IS IMPORTANT

The Payment Card Industry Data Security Standards (PCI DSS or just PCI) was created by the Payment Card Industry Security Council for the purpose of protecting cardholder data that is being processed, stored or transmitted by merchants. The security controls and processes that make up the PCI DSS are critical to providing protection to the customer's cardholder data.

1.2 WHAT IS CARDHOLDER DATA

Cardholder data at a minimum refers to the name on the credit card account and any of the information about the card that refers back to the account. Sensitive items include (but are not limited to): Account number, Expiration date, Personal data provided by the guest, and other data gathered by our organization to process the transaction. Cardholder data may be found either visually on the card or electronically on the magnetic stripe or through a computer chip embedded in some cards.

1.3. SENSITIVE AUTHENTICATION DATA

Cardholder and Sensitive Authentication Data should never be stored in any format. In the normal course of day-to-day business **if an employee can see more than the last four digits of the Primary Account Number (PAN - sixteen digit Credit Card Number) displayed, it is every employee's responsibility to report this immediately to upper management.** Management will make every effort to correct this situation and expects to be notified if credit card information is ever exposed.

Granite City Food & Brewery/Cadillac Ranch has made every effort to select secure systems to protect our customer's sensitive Credit Card data. These systems process Credit Card transactions that retain that information for the purpose of business, legal or regulatory purposes only. These systems should not display cardholder data or store sensitive authentication data in a non-compliant manner. If any employee suspects the wrongful performance of the software, the transmission of Credit Cards, Sensitive Authentication Data, sensitive guest information, employee, or company secrets, it should be reported immediately.

Sensitive Authentication Data elements which must be protected are:

1. **Full Magnetic Stripe:** There are two tracks of data on a bankcard's magnetic stripe found on the back of the credit card.
    a. Track 1 is 79 characters in length, is alphanumeric and contains the account number, the cardholder name, and the additional data listed on Track 2.
    b. Track 2 is the most widely read, is 40 characters in length and is strictly numeric. This track contains the account number, expiration date, secure code, and discretionary institution data.
2. **CVV (Card Verification Value):** such as, CAV2/CID/CVC2/CVV2 – Card Identification found on the back of a Discover, JCB, MasterCard or Visa card (3 digit number)
   PIN/PIN Block: Personal Identification Number that is an alphabetic or numeric code that may be used as a means of card holder identification typically used for debit card transactions.

1.4 WAYS TO PROTECT CARDHOLDER DATA

1. Never store Cardholder Data or Sensitive Authentication Data electronically.
2. Do not copy cardholder data or Sensitive Authentication Data on any form of media electronically.
3. Do not write down Cardholder Data or Sensitive Authentication Data.
4. Do not email or use any other electronic means to transfer cardholder data or Sensitive Authentication Data under any circumstances. If you receive cardholder data via email it must be deleted immediately and the cardholder must be notified that it is against policy to accept credit card data in emails and ask that they do not send in email in the future due to the company's inability to protect their data.
5. In the event you are handed a credit card to complete a transaction, make certain that you hand the guest their credit card back and thank them for their business.
6. **If a customer leaves their credit card behind, notify management immediately.** Management will secure the card and contact the guest if possible. If the customer does not return for their card within 24 hours it will be destroyed per company policy. If the guest returns or calls after 24 hours, notify them that the card was destroyed to protect their account security.

2. Approved Crash Kit Process

During the normal course of business electronic and automated systems may not work as planned. For example, credit card processing or the Point-of-Sale may be temporarily offline. If this occurs, notify management immediately so that repairs are initiated.

If the credit card processing is offline and the Point-of-Sale functions properly, all credit cards should be entered using stand-alone procedures. This will allow you to continue to enter credit cards into the system and they should automatically process when the credit card processing comes back online.

Manual imprinting or other means of written card transaction are not allowed.

3. Security Fraud Awareness {Cyber Crime}

While Granite City Food & Brewery/Cadillac Ranch has custody of the guest's credit card account information, as a representative of the company, it is your responsibility to ensure that you do everything possible to keep their information safe and secure. Today cybercrime rings are active and working hard to find sensitive data that can be used to their financial benefit. This is a real threat and we are committed to conducting business in the most secure means possible. The following information is provided is not all inclusive but should provide a basic awareness of possible threats.

3.1 MALWARE

Malware is harmful software such as viruses or Trojans designed to cause damage or disruption to a computer system. Cyber criminals may try to install malware for the purpose of collecting Cardholder Data or Sensitive Authentication Data to sell on the black market. For this reason, all computer systems that have access to sensitive cardholder data must be running anti-virus software that can detect and eliminate known forms of malware.

1. **Through email**: many malware programs are distributed through email. Never open email from an unfamiliar source.
2. **Through browser**: many malware programs can be automatically downloaded by clicking on an unsecure website page or popup. Never access unapproved websites from any machine that is involved with processing credit cards or that has customer data.
3. **By connecting**: with an unsecure connection or to an unsecure environment via websites or remote access. Never access other network environments without prior approval from management, and report suspicious behavior on the computer systems to management.
4. **By installing unapproved programs**: many malware programs are included with what appears to be harmless applications or freeware. Never download any application into the computer environment at work without prior approval from management.

3.2 EMAIL

Email Viruses

Email viruses may spread through email attachments, file sharing, downloading files or software, Instant Messaging (IRC, ICQ, etc.), portable disks, and web pages. If you ever receive an e-mail message that has a suspicious attachment (a program, document, picture or sound file) that you were not expecting, do not open the message or the attachment. Delete it and verify with your IT technical support contact that your system has not been compromised.

Email Spoofing

Email spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used for spam email and phishing to hide the origin of an email message. **If you suspect that you are receiving spoofed messages contact management.**

Email Attachments

Attachments to email messages can contain viruses and other malware. If you receive any of the following as attachments to an email, do not open the attachment:

- ☑ .exe such as *sample.exe* or *whatever.exe*

- ☑ any email attachment with two file extensions such as *resume.doc.pif* or *win-free-stuff.txt.vbs*
- ☑ any email attachment with file extensions: *.bat*, *.reg*, *.scr*, *.dll* or *.pif*
- ☑ any email or attachment that asks you to delete files from your hard drive

Email Spam
Always protect your work email address. Never distribute your work email address to non-business related personnel or websites. Unscrupulous websites will distribute your e-mail address to cyber thieves who will attempt to penetrate our systems with the dangerous e-mails listed above.

Email Use
Email and company networks are to be used for business purposes only. Access to non-corporate email is against company policy and should be totally avoided while using a company computer. Furthermore, if you receive cardholder data via email it must be deleted immediately and the cardholder must be notified that it is against policy to accept credit card data in emails. Ask the sender to not send them in the future due to the company's inability to guarantee that such data would be protected. Management has the right to capture or monitor any communications or network activity that occurs in the company environment.

3.3 WEB BROWSER

Company networks are to be used for business purposes only. Only the corporate approved web browser should be used. Do not install any additional web browsers, upgrade the existing web browser, or replace the existing corporate approved web browser. Always avoid ad ware and spy ware. Always ignore ads that may compromise your computer or get you to install an illicit program. Never click on pop ups.

3.4 PHYSICAL THEFT

Any employee involved in activities involving credit card data theft is subject to termination and possible criminal prosecution. These activities are serious crimes and are often prosecuted as felonies.

Skimming
One of the most common methods for a thief to obtain credit card data is by the use of a "skimming" device. These devices are small magnetic stripe readers that can easily be purchased online along with a keystroke catcher. These devices are legitimate transaction devices typically used in gyms and can be as small as a lighter. Employees at restaurants can accomplish this in a quick second. These numbers are then sold to cybercrime rings. It is your responsibility to report any suspicious activity to management.

Manual Credit Card Data Capture
Another method of credit card theft is to manually write down the credit card information for use or resell at a later time.

Social Engineering
In a social engineering attack, the attacker uses their social skills to take advantage of the human tendency to trust someone on their word. These deceptions are created for the sole purpose of extracting sensitive data or achieving physical access to an otherwise secure area. Always contact management for approval if anyone requests sensitive information from you. Finally, your username and password should never be given out.

Another method of trickery is to provide a free electronic storage device or simply leave a device where an unsuspecting user will insert the device out of curiosity to determine what is on the drive. Never insert or allow anyone else to insert an unknown or non-company sanctioned storage device into a company system.

4. Acceptable Use Policy

4.1 OVERVIEW & PURPOSE

Granite City Food and Brewery/Cadillac Ranch's intentions for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to Granite City Food and Brewery/Cadillac Ranch's established culture of openness, trust and integrity. Granite City Food and Brewery/Cadillac Ranch is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, and internet browsing are the property of Granite City Food and Brewery/Cadillac Ranch. These systems are to be used for business purposes in serving the interests of the Company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This policy outlines the proper use of employee-facing technologies, including wireless, modems and remote access technology. All employees and contractor personnel that have access to organizational computer systems and networks must adhere to the acceptable use policies defined below in order to protect the security of the network, cardholder data, computer systems, and data integrity.

This policy applies to employees, contractors, consultants, temporary and other workers at Granite City Food and Brewery/Cadillac Ranch, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Granite City Food and Brewery/Cadillac Ranch.

4.2 GENERAL USE & OWNERSHIP

While Granite City Food and Brewery/Cadillac Ranch desires to provide a reasonable level of privacy, users should be aware that the information they create or access on Company systems remains the property of Granite City Food and Brewery/Cadillac Ranch. Because of the need to protect the Company's network, and cardholder data, management cannot guarantee the confidentiality of information developed by employees and stored on any network device belonging to Granite City Food and Brewery/Cadillac Ranch.

Granite City Food and Brewery/Cadillac Ranch, in its routine management of the business, shall conduct the following IT oversight activities:

1. For security and network maintenance purposes, authorized individuals within Granite City Food and Brewery/Cadillac Ranch may monitor equipment, systems and network traffic at any time.
2. Granite City Food & Brewery/Cadillac Ranch reserves the right to audit networks and systems on a periodic basis (at least annually) to ensure compliance with this policy.

Such audits will be used to determine if additional policies are necessary to mitigate additional risks.

3. Any device that connects to or accesses Granite City Food and Brewery/Cadillac Ranch network that has access to cardholder data, must be inventoried and approved by Company management.

4.3 USE OF REMOTE ACCESS OR WIRELESS TECHNOLOGY

The use of any remote access or wireless technology to access any Company system or processing resource which is within the cardholder data environment or contains any cardholder data, whether at service provider hosting locations or Company locations, requires the explicit written approval of an Executive Manager of Granite City Food and Brewery. Such access is otherwise specifically prohibited.

However, should permission be granted to any employee or contractor to use remote access or wireless access to cardholder data or the cardholder data environment, then the following policies and procedures shall be followed:

- ☑ Automatic disconnect of remote access sessions after 5 minutes of inactivity for any user shall be invoked.
- ☑ Wireless connectivity shall be logged and monitored to protect the cardholder data environment.
- ☑ Activation of remote access for vendors shall be strictly limited to the amount of time that is needed by vendors, with immediate deactivation after use.
- ☑ When accessing cardholder data remotely via approved remote access methods, Granite City Food and Brewery shall prohibit storage of cardholder data onto local hard drives, floppy disks, or other external media; and prohibit cut-and-paste and print functions during remote access unless it is for a justified business purpose which has been specifically approved by management before such technology is enabled.
- ☑ Wireless intrusion scans shall be performed in accordance with the current PCI DSS standards.

4.4 PROTECTION OF PROPRIETARY & SENSITIVE DATA, INLCUDING CARDHOLDER DATA

The user interface for information contained on Internet/Intranet/Extranet should protect confidential information which includes but is not limited to: company private data, job applications, human resource documentation, corporate strategies, cardholder data, trade secrets, and specifications. Employees should take all necessary steps to prevent unauthorized access to this information.

Any Company system that stores, transmits, or processes cardholder data must have management approval prior to being connected to Granite City Food and Brewery network. Furthermore, only systems that are specifically authorized on Granite City Food and Brewery's list of approved software and hardware are eligible for connection to Granite City Food and Brewery's credit cardholder data environment. This list includes the manufacturer/publisher, model/edition, and other specifications as appropriate. Storage of cardholder data is discouraged to limit unauthorized access to cardholder information. Storage of cardholder data on local drives is prohibited. When storage or displaying of cardholder data is required, the Primary Account Number (PAN) must be encrypted or masked displaying either the first six or last four numbers. Full track data shall never be stored or displayed on any device. Notify management if you find evidence otherwise during the normal course of business. **Notify management if you discover cardholder data stored on local drives, the PAN not encrypted or masked, and/or full track data stored or displayed on any device.**

Wireless access to Granite City Food and Brewery network must be encrypted with WPA or WPA2 encryption. Wireless access to Granite City Food and Brewery network must be segmented from cardholder data behind a firewall if access has been approved by appropriate management.

A good data protection plan also includes updating and patching all system components with the latest vendor-supplied security patches. It is the policy of Granite City Food and Brewery to install critical security patches within 30 days of their release. **Notify management if you believe that a system component does not have the latest vendor-supplied security patch or if you observe a warning message pertaining to patches in an application.**

5. Unacceptable Use

The following activities are, in general, prohibited. Employees or contractors may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Granite City Food and Brewery or a contractor authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Company-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.1 UNACCEPTABLE SYSTEM & NETWORK ACTIVITIES

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Granite City Food and Brewery.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Granite City Food and Brewery or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Company Name computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Granite City Food and Brewery account.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, skimming and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless specifically requested by management.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
13. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
14. Providing information about, or lists of, Company employees to parties outside Granite City Food and Brewery.
15. Writing down sensitive information such as Cardholder or Sensitive Authorization Data and removing from Company premises or using for personal gain or using stolen Cardholder data on Company systems for personal gain.

6. Information Security Policy

6.1 WHY INFORMATION SECURITY

1. Information Security helps to:
2. Safeguard GCFB's assets and those belonging to our customers, third-parties, employees, and other entities.
3. Support GCFB's compliance with regulations, standards, and/or laws.
4. Reduce risk to GCFB's assets.
5. Support the integrity of information and data.

6.2 USAGE OF GCFB ASSETS

GCFB's assets may only be used to support GCFB business and operations. Users may not use GCFB assets for personal use, unless authorized by their manager. Use of GCFB assets must always be in a professional manner.

The following actions are never permitted when using GCFB assets:

1. Compromising confidentiality, integrity, and availability of GCFB assets.
2. Threatening, obscene, profane, offensive language or content.
3. Harassing or violating others.
4. Gaming, file sharing, music, and other activities.
5. Work for another business, commercial venture, or non-GCFB- sponsored activities.
6. Advertising, purchasing, selling, and transacting non-GCFB initiatives.
7. Any illegal activities.

6.3 NO EXPECTATION OF PRIVACY

Users are to expect that GCFB may access or view their actions using GCFB systems at any time and without prior notification. GCFB reserves the right to disclose any user actions and communications to law enforcements or other parties without prior consent from the user.

6.4 LEGAL AND COMPLIANCE REQUIREMENTS

GCFB is required to comply with several regulations, standards, and/or laws for our own organization, to meet our third-party contractual requirements, and also perhaps on behalf of our customers' compliance efforts.

GCFB is required to comply with:

Payment Card Industry Data Security Standards (PCI DSS): Industry requirements put forth by the card brands and acquirer banks to safeguard cardholder data>

Sarbanes-Oxley Act (SOX): Security of information supporting internal control structures for financial reporting>

State Data Privacy/Breach Notification Laws: Legislation requiring organizations to notify individuals or entities when there are breaches involving personal information. A current list of state laws is maintained at http://www.clla.org/documents/breach.xls

6.5 ROLES AND RESPONSIBILITIES

Users are required to:

1. Follow GCFB policies at all times.
2. Help GCFB meet and maintain compliance with this Information Security Policy.
3. Acknowledge their agreement with this Information Security Policy before their first access to GCFB's assets and then annually for the lifetime of their access.
4. Be aware of their role in supporting GCFB's information security program.
5. Comply with relevant regulations, standards, and/or laws governing GCFB and GCFB's customers, third-parties, and other applicable entities.
6. Safeguard GCFB's assets per the policies within this Information Security Policy.
7. Report any deviation from this Information Security Policy to their direct manager immediately.

Managers are required to:

In addition to the above requirements:

1. Ensure that their reports follow GCFB policies at all times and understand their roles.
2. Designate owners (if not themselves) for GCFB assets under their control and management.
3. Work with other groups to implement and maintain security controls for assets.

4. Participate (as needed and directed) in incident response procedures.

Asset Owner/Managers are required to:

In addition to the above requirements:

1. Manage the definition of user access to the assets under their control and management.
2. Ensure that user access to their assets follows the principle of "least privileges".
3. Verify that assets are protected sufficiently with the security controls.
4. Properly assess and classify assets.
5. Appoint a backup for when they are unavailable.

IT Department Employees are required to:

In addition to the above requirements:

1. Oversee and manage compliance with GCFB's policies.
2. Perform risk assessments.
3. Evaluate and select solutions to reduce risk to GCFB assets.
4. Write and distribute security policies to all users (as defined in the Introduction).
5. Monitor and analyze security alerts and information and distribute to appropriate personnel.
6. Define and deploy incident response and escalation procedures.
7. Administer user accounts, including additions, deletions, and modifications.
8. Monitor and control all access to data.
9. Develop and implement Security Awareness and Training programs.
10. Receive alerts from users and other systems 24/7/365.
11. Provide direction to management on best security practices and recommended security controls and initiatives.

Senior Management is required to:

In addition to the above requirements:

1. Champion best security practices from a "top down" approach.
2. Take ultimate responsibility for safeguarding GCFB's assets.
3. Accept residual risk resulting from assessment initiatives.

7. Information Security Policy

7.1 ACCESS CONTROL

Without defined access privileges and control, users would be allowed to access systems and applications in GCFB's cardholder data environment, and be able to view, delete, and tamper with stored data, code, and configurations. Therefore, controlling who has access to what and

what actions they are permitted to perform is important to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access.

A careful review of each system and application should be performed based on results from risk assessment activities performed by GCFB, and user's granted access privileges based upon the principle of "business need-to-know" (where access is based on whether the individual requires access based upon their function or role). The general rule to follow is that all users start with no access privileges and are granted access to systems, applications, tools, etc. individually, as needed. All access granted is to be tracked in <method/form>, and reviewed on a quarterly basis as users may; leave the company, temporarily need access to specific systems, or, change positions where they no longer require access privileges.

Reference: Access Management Policy.

7.2 ANTI-VIRUS

Viruses, and associated spyware, adware, and malware, can infiltrate GCFB's network, causing incalculable damage to systems and applications transmitting, processing, and/or storing sensitive data.

Viruses can shut down complete systems; spyware can capture user actions and take screenshots of cardholder data; and malware can spread through your network, causing damage to GCFB, customers, and third-parties.

Anti-virus software must be deployed on all corporate servers, workstations, and gateways that are considered to be those commonly affected by viruses. This means that Unix-based systems may not require anti-virus to be deployed. Anti-virus software for Unix is available so GCFB should determine whether it would be recommended to deploy such software for these systems based upon risk assessment results. The anti-virus software should be an up to date/current enough version that it protects against spyware and adware.

Reference: Anti-Virus Policy.

7.3 BACKGROUND CHECKS

The level of risk associated with a user containing a prior criminal record may be higher than for a user with no such record on a general basis. Just as it's important to reduce the level of risk from access to systems and applications transmitting, processing, and/or storing sensitive data, performing background checks on the users with such access is important and required.

Background checks are to be performed minimally on all users with access to systems and applications transmitting, processing, and/or storing sensitive data, and optimally on all GCFB employees. Results from the background checks are to be reviewed and accepted prior to the user being granted access to the environment. The GCFB IT Dept. with the HR Dept. should determine the level of acceptance of background check results prior to checks being performed on users. For example, a user with a recent history of criminal theft may be regarded differently than a user with a minor infraction from twenty years ago. These criteria should be communicated to individuals prior to the check performed. Background checks should also be required of third-parties requiring access, whether temporarily or permanent. Background checks are to be performed following local and national laws.

Reference: Background Checks Policy.

7.4 CHANGE MANAGEMENT

Performing changes to systems and applications in GCFB's environment carries some level of risk, whether the change is a simple code change or applying the latest critical patch to a complete system reconfiguration. Attackers are aware of lax (or simply incorrectly performed) change control processes performed by organizations and have created specific attack methods which would allow them to take advantage of vulnerabilities to successfully penetrate systems and applications transmitting, processing, and/or storing sensitive data.

Subsequently, changes should be made only when absolutely necessary and managed closely from inception to deployment into the production environment, complete with backout plans in case the change creates vulnerability.

Reference: Change Management Policy.

7.5 CRITICAL TECHNOLOGIES

Critical technologies include remote access, wireless, removable media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage. These are all tools used to access GCFB's network in a "non- standard" method, meaning they can be used remotely and not use a GCFB workstation in a GCFB location. Special care should be made when using these technologies as they are accessing GCFB's network from an unknown location, therefore safeguarding the connection to the network is critical. It's also important to limit actions, which users can take, using these technologies to protect cardholder data wherever it is transmitted, processed, and/or stored.

Reference: Critical Technologies Policy.

7.6 DATA CLASSIFICATIONS

The purpose of classifying data is to be able to define and implement the appropriate level of security controls to protect it from unauthorized access and use. The higher the level of classification, the more intensive and comprehensive the security controls should be in place to protect it. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment.

Printed and electronic data is to be classified in terms of its value to GCFB, sensitivity, legal requirements, and impact if it is lost or falls into the 'wrong hands'. When performing a data classification exercise, it's critical to review the methods in which this data can be transmitted, stored, or used. Electronic data can be emailed, faxed, transmitted via instant message and/or other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, backup tapes, and similar. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Critical Data

This type of classification is assigned to assets and data sets which, if lost, would cause serious harm to GCFB, GCFB's customers, GCFB's third-parties, and others. Harmful affects can be from a financial, competitive, compliance, legal, branding, and/or reputation perspectives. Subsequently, it must be kept confidential.

Examples include cardholder data, financial plans, business and strategic plans, and customer lists.

Private Data

This type of classification is assigned to assets and data sets which, if lost, could potentially cause harm to GCFB, GCFB's customers, GCFB's third-parties, and others; however it would not be unrepairable. Subsequently, it should be kept confidential as much as possible.

Examples include intranet content, performance evaluations, and internal communications (unless they contain confidential information).

Public Data

This type of classification is assigned to assets and data sets which are readily available and part of the public domain so would not cause any harm to GCFB, GCFB's customers, GCFB's third-parties, and others. Subsequently, it does not require specific security controls.

Examples include GCFB's website, marketing materials, press releases, and external announcements.

Reference: Data Classification Policy.

7.7 DATA DISPOSAL

Assets and data sets need to be safeguarded from unauthorized access and use throughout the lifecycle. When no longer needed for business reasons, care should be taken to ensure that the asset and its data cannot be accessed or regenerated by an unauthorized user when disposed of or transferred to a new party. Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment.

Secure disposal and deletion methods are required for assets and data sets which are classified as <Confidential> or Private Data. Items classified as Public Data may be reused freely.

Disposal Requirements for Electronic Data on:

Assets Labeled as Critical Data

Critical Data assets are to be securely wiped using an industry-strength wiping tool or format prior to being transferred to another party. If the asset is not going to be reused, the item should be physically destroyed in addition to taking the extra precaution of being securely wiped. Checks should be made of each asset to ensure that the data has successfully been deleted prior to the asset being provided to another party. The deletion or destruction schedule should

be documented and reviewed by GCFB IT Dept. on a quarterly basis. Users should be made aware of the importance of safely destructing and deleting these assets and data.

Cardholder data must be securely erased when it no longer meets its retention requirements (see
Data Retention Policy). If this period of time is longer than 90 days, an audit must be performed on a quarterly basis to ensure that it has not exceeded its defined retention period.

Assets Labeled as Private Data

Private Data assets are to be securely wiped and/or physically destroyed, and recorded, in the same manner as for those labeled as Critical Data.

Assets Labeled as Public Data

Public Data assets are not required to be securely wiped using an industry-strength wiping tool or format prior to being transferred to another party; however it is recommended as a best practice. If the data is not securely deleted, then checks of each asset must be made to ensure that there is no sensitive data retained prior to the asset being provided to another party. The deletion or destruction schedule should be documented and reviewed by GCFB IT Dept. on a quarterly basis.

Disposal Requirements for Printed Data:

Labeled as Critical Data

Printed documentation labeled as Critical Data assets are required to be shredded using a cross-cut shredder. All areas handling documentation with sensitive information must have such a shredder located nearby or a locked bin if a third-party is used to pick up the documentation for shredding. These documents are to be securely retained up to their destruction. Third-party vendors used to shred documentation must have provided a signed Non-Disclosure Agreement and agree to GCFB's terms and conditions of protecting the sensitive data. The destruction schedule should be documented and reviewed by GCFB IT Dept. on a quarterly basis. Users should be made aware of the importance of safely destructing these documents.

Cardholder data must be securely destructed when it no longer meets its retention requirements
(see Data Retention Policy). If this period of time is longer than 90 days, an audit must be performed on a quarterly basis to ensure that it has not exceeded its defined retention period.

Assets Labeled as Private Data

Private Data assets are to be destroyed, and recorded, in the same manner as for those labeled as Critical Data.

Assets Labeled as Public Data

Public Data assets are not required to be securely destroyed. If the data is not securely deleted, then checks must be made of each asset to ensure that there is no sensitive data retained prior to the asset being provided to another party. The destruction schedule should be documented and reviewed by GCFB IT Dept. on a quarterly basis.

Reference: Data Disposal Policy.

7.8 DATA HANDLING

Assets and data sets need to be handled by users according to their classification in order to properly safeguard it from unauthorized access and usage (see Data Classification Policy). Data can be in electronic or printed format, and may be transmitted, processed, and/or stored in the cardholder environment. GCFB's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

Electronic data can be emailed, faxed, transmitted via instant message and other messaging technologies. Printed data can be faxed, hand delivered, scanned, and mailed. Data can be stored on systems, in code, workstations, devices, mobile media, backup tapes, and others. Electronic data can be printed or copied to another workstation or system. Printed data can be retained in file cabinets and on desks.

Handling Requirements for Assets and Data Sets Labeled as Critical Data:

Changes:	Changes made to these assets and data sets must be approved by GCFB IT Dept. and the system owner prior to the change, recorded and retained for minimum of one year.
Email:	Only individuals approved by GCFB IT Dept. to transmit this data may do so, and then only if the email and its attachments are approved using a GCFB-approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non-GCFB email system or posted/ communicated via the Internet. This includes posting to websites or using Internet email and messaging technologies.
Fax:	The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
Internal Mail:	This type of data should not be delivered over internal GCFB mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.
External Mail:	This type of data is to be packaged in a secure manner and delivered by a commercial delivery service that can be tracked. A return receipt should be used or requested, such as a delivery signature.
Printing:	This type of data should not be printed unless absolutely needed for business purposes, and after approval from the GCFB IT Dept.. The printing must be supervised.
Print Storage:	Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.

Electronic Storage: Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a GCFB-approved method. This includes data storage on workstations, systems, etc.

Handling Requirements for Assets and Data Sets Labeled as Private Data:

Changes: Changes made to these assets and data sets must follows the GCFB Change Management Policy.
Email: Only individuals approved by GCFB IT Dept. to transmit this data may do so, and then only if the email and its attachments are approved using a GCFB-approved encryption method. A receipt request should be used or requested.
Internet: This data may never be transmitted using a non-GCFB email system or posted/ communicated via the Internet. This includes posting to websites or using Internet email and messaging technologies.
Fax: The person sending the fax with this data is required to be present at the fax machine to verify that it has been sent and is not stored in the memory. A receipt request should be used or requested.
Internal Mail: This type of data should not be delivered over internal GCFB mail, unless absolutely necessary and then a return receipt should be used or requested. It is preferable to deliver the item in-person.
External Mail: This type of data is to be packaged in a secure manner and delivered by a commercial delivery service that can be tracked. A return receipt should be used or requested, such as a delivery signature.
Printing: This type of data should not be printed unless absolutely needed for business purposes, and after approval from the GCFB IT Dept.. The printing must be supervised.
Print Storage: Printed data is required to be within eyesight or within possession at all times, or locked up in a secure manner or location.
Electronic Storage: Stored data may not be retained in a readable format and is to be truncated, masked, or encrypted using a GCFB-approved method. This includes data storage on workstations, systems, backup tapes, etc.

Handling Requirements for Assets and Data Sets Labeled as Public Data:

Access: Access is available to everyone
Non-Disclosure (NDA): No NDA is required to distribute these assets or data
Changes: Changes should follow the Change Management Policy
Email: May be readily emailed
Internet: May be readily transmitted; however caution should be used if posting to an external website to ensure that GCFB's reputation will not be harmed.
Fax: May be readily faxed
Internal Mail: May be delivered freely via internal mail
External Mail: Mail be readily mailed outside of GCFB
Printing: May be readily printed
Print Storage: Does not need to be stored securely
Electronic Storage: Does not need to be stored securely

Reference: Data Handling Policy.

7.9 DATA RETENTION

The retention period for assets and data sets may be affected by legal, industry, financial, and/or regulatory requirements. In order to reduce risk, however, assets and data sets should not be retained longer than absolutely required in the cardholder environment.

Each asset and data set (both electronic and printed formats) should be reviewed by a Legal point-of-contact to assess GCFB's legal, industry, and regulatory requirements for its length of retention. The same exercise should be performed by the system owner as well as management to assess its industry requirements for retention. When completed, an analysis should be performed with the guiding principle that the item should be retained for the least amount of time as is possible.

Reference: Data Retention Policy.

7.10 EQUIPMENT PROTECTION

Equipment (to include systems and cabling) supports day-to-day operations of systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data. Should the equipment be subjected to harsh conditions, intended or unintended misuse, liquids, or other types of physical hazards and/or threats, its ability to function may be impacted, subsequently impacting the security of the environment.

Food and beverages may not be brought into data centers or computer rooms at any time, or within <proximity> of GCFB equipment.

Reference: Equipment Protection Policy.

7.11 FILE INTEGRITY

File integrity software is used to ensure that no modifications have been made to content files, operating system critical files, executables, configuration files, and audit logs for systems and applications transmitting, processing, and/or storing sensitive data. File integrity software must be used on all systems responsible for/involved in transmitting, processing, and/or storing cardholder data in the following places/functions:
Content files
Operating system critical files
System and application executables
System and application configuration files
System audit log files

Reference: File Integrity Policy.

7.12 FIREWALL CONFIGURATION AND MANAGEMENT

Firewalls are critical to safeguard GCFB's cardholder data environment as they filter access to systems and applications transmitting, processing, and/or storing this sensitive data.

Firewalls utilize established rule sets to allow or deny inbound or outbound network traffic between trusted and untrusted environments. Trusted environments include known zones that contain systems which transmit, process, and/or store cardholder data, and the internal network in general. Untrusted environments include Internet-facing access points, unknown environments, wireless networks, and zones which do not contain such systems which transmit, process, and/or store cardholder data. Firewalls are required to be placed at any Internet connection (to protect against traffic coming in from outside of GCFB) and between internal network zones (should one zone contain sensitive systems and the other does not).

Reference: Firewall Configuration and Management Policy.

7.13 INCIDENT RESPONSE

Security controls work together to reduce risk in GCFB's environment. These controls include intrusion detection systems, file integrity software, firewalls, logging, and many others. Many of these security controls are also used to notify the GCFB IT Dept. whenever a suspected incident takes place or there is a system anomaly detected in GCFB's cardholder environment. This allows the GCFB IT Dept. to respond to and perform necessary activities to limit damage being caused. GCFB users also play an important role in supporting the incident response process, by reporting anomalies they are encountering, such as a suddenly slower computer, accidental viewing of cardholder data in the clear, or a lost removable computer drive.

Reference: Incident Response Policy.

7.14 INTRUSION DETECTION/PREVENTION

An Intrusion Detection/Prevention System (IDS/IPS) detects suspected intrusions from the outside (if the attacker has managed to bypass the firewall) or originating from the network, logs the event, and generates an alert. The IDS/IPS perform their function relying on updated signatures, which are patterns of common attacks, from the IDS/IPS vendor. Using these signatures, the IDS/IPS can then detect intrusions which follow those patterns before they can cause damage to systems and applications transmitting, processing, and/or storing sensitive data.

IDS differs from IPS where the former simply detects the suspected intrusion and sends an alert, but the latter actually responds to the attack by stopping it, reconfiguring the firewall, or disabling it. PCI requirements are that there is 24/7/365 response to suspected intrusions and attacks. If using an IDS, a member of the GCFB IT Dept. needs to respond immediately to the suspected event and perform forensic, remediation, and then investigative follow-up initiatives. Should an IPS be deployed, the GCFB IT Dept. needs to ensure that the attack has been blocked and perform investigative follow-up.

Reference: Intrusion Detection/Prevention Policy.

7.15 LOG MANAGEMENT

Logging enables GCFB to know who logged on to a system and when, and what actions did the user or application do. This is important to proactively monitor access to cardholder data and to identify anomalies, and also to review access should there be concern of an incident or breach to cardholder data being transmitted, processed, and/or stored.

Logging should be enabled on all systems where it is feasible to do so, which includes databases, servers, user's desktops, applications (as applicable), networking equipment, wireless access points, etc.

Reference: Log Management Policy.

7.16 PASSWORD MANAGEMENT

Passwords are the most common method of authenticating the identity of the user before allowing access to systems and applications in GCFB's cardholder data environment. Subsequently, the effective management of user passwords is critical to support systems and applications transmitting, processing, and/or storing sensitive data from unauthorized access.

The user is responsible for constructing strong passwords, following GCFB policies, and protecting the secrecy of their password. The GCFB GCFB IT Dept. is responsible for enforcing password parameters using automated access control methodologies, to include the required length of passwords, reuse, lockouts, history, change upon first login, secure storage, and other security controls. In addition, the GCFB GCFB IT Dept. is responsible for deploying additional authentication methods as defined by GCFB GCFB IT Dept. resulting from risk assessment activities (i.e: two-factor authentication for remote access or for privileged access to critical systems and applications).

Users may not share their passwords with any other parties, even at their direct request. The user should notify the GCFB IT Dept. should they receive a request for their password to initiate the incident response plan. In addition, users must take additional precautions to protect the security of their passwords by not writing it down, making it something which is readily known, or keeping it stored in an accessible location.

Users should not write down their passwords or store them electronically, unless using a pre-approved password storage system. In addition, users may not 'cache' or select an option to remember their password when online, as this may store the password insecurely. The GCFB IT Dept. must store user passwords in a secure manner, protected from unauthorized access and in unreadable format.

Reference: Password Management Policy.

7.20 PHYSICAL SECURITY

An unauthorized person may cause physical damage to GCFB's cardholder environment, which can lead to assets and data being used inappropriately.

An individual may socially engineer their way into the facility, meaning, pretend to be an authorized individual or trick an employee into letting them in under false pretenses. Once inside, the individual may continue to ruse others into granting them continued physical access to secured locations or even logical access to systems and data.

All persons entering, or in the environment of, any of GCFB's facilities or locations which transmit, process, and/or store cardholder data must follow these physical protection policies.

The identity of all individuals accessing facilities and locations transmitting, processing, and/or storing cardholder data must be verified prior to their entrance. All Visitors must provide evidence of their identity and be approved by a GCFB Manager prior to being granted access to the facility. Visitors are to be accompanied at all times, unless specifically authorized by GCFB IT. All Visitors requesting access to Computers, Network equipment or any other networked devices, must be pre-approved by the GCFB IT Dept.

All employees are to wear GCFB approved uniforms. Uniforms and personal recognition are to be used in place of badges. All visitors the GCFB restaurants are to be considered Visitors. The visitor may not be granted access privileges to areas which transmit, process, and/or store cardholder data, unless specifically authorized by GCFB IT. Visitors must sign in and out each time they are granted access to areas which transmit, process, and/or store cardholder data. The employee that is authorizing their presence is responsible for ensuring that the visitor is accompanied and signing in and out of the secured area. Employees should feel empowered by management and trained to ask any individuals who not uniformed GCFB employees as to their purpose in the building.

Logs are to be recorded and retained for both the visitor's entrance into secured areas which transmit, process, and/or store cardholder data. The logs are to record the person's name, company, purpose, employee visiting/authorizing the visit, and date and time. The logs are to be retained for a minimum of 365 days.

Reference: Physical Security Policy.

7.21 RISK ASSESSMENT

The purpose and intent of GCFB's security program is to reduce risk as much as possible to GCFB's environment, while still enabling GCFB to meet strategic and business objectives. Defining the risk level of assets (systems, equipment, applications, data, users, etc.) is critical in order to define the level of security controls required to safeguard those assets from harm. As it is impossible to reduce risk to zero, there will always be an amount of residual risk left. It is up to GCFB <Senior Title> to review and accept this level of risk. The higher the risk level associated with an asset, the more intensive and comprehensive the layers of security protecting the asset are required for cardholder data being transmitted, processed, and/or stored.

Reference: Risk Assessment Policy.

7.22 ROUTER CONFIGURATION AND MANAGEMENT

Routers are an integral part of GCFB's network to safeguard GCFB's cardholder data environment as they direct traffic to systems and applications transmitting, processing, and/or storing this sensitive data.

Routers route traffic will be based upon internal addresses and defined route tables to ensure that it arrives at its intended destination. Routers may also assist with functions performed by the firewall(s) where certain data packets are blocked. Subsequently, the protection of the router and of its configuration file is important in order to protect against external traffic being transmitted into trusted environments that contain systems which transmit, process, and/or store cardholder data, and the internal network in general.

Reference: Router Configuration and Management Policy.

7.23 SECURE CONFIGURATION

As demands on time, productivity, and operations increase, the focus on securely configuring systems and network devices may suffer a lack of attention or a heightened amount of exceptions granted. Common security vulnerabilities, such as default passwords not being changed or a port remaining open after an exception request expires, can open up holes for an individual to gain unauthorized access to systems and applications transmitting, processing, and/or storing sensitive data.

Each system and networking component should be included in the annual risk assessment performed by GCFB, GCFB IT Dept., and their configurations compared against documented best security practices and standards. These documents should keep a record of the baseline configuration of the system and network component and deviations reviewed on a quarterly basis to ensure that risk cannot be introduced into the environment.

Reference: Secure Configuration Policy.

7.24 SECURITY AWARENESS

Breaches can often be attributed to the actions performed by an organization's employee(s), whether they are intentional or unintentional. If people are not provided with awareness of their roles and responsibilities when it comes to protecting GCFB's assets and data, they cannot be held responsible for their actions or know how their actions impact the security of GCFB's cardholder environment.

Users must receive security awareness training and sign an acknowledgment of their role in safeguarding GCFB prior to being granted physical and logical access to GCFB's environment.

All users, for the entire length of time they are, or remain, connected to GCFB's environment, must receive security awareness training on an annual basis. This training may be provided to all users at one time, or may be staggered to take place on an annual basis from the user's first day of employment or access granted. Training may occur in-person or via a computer-based training (CBT) format.

Attendance logs for those who attend security awareness training, both, provided upon hire and annually, must be kept by the GCFB IT Dept.. Exceptions must be communicated to the user's manager with a defined period of time that the user must take the training. Should the user not take the refresher training within that period, they are to be found in violation of this policy.

All users, for the entire length of time they are, or remain, connected to GCFB's environment, are to sign an agreement with GCFB's terms and conditions and acknowledgment of their role in safeguarding GCFB's environment on an annual basis. This should also occur when the security refresher training is provided.

Reference: Security Awareness Policy.

7.25 TESTING AND SCANNING

Testing GCFB's systems and network is a critical component of protecting GCFB's cardholder environment from threats and vulnerabilities.

New vulnerabilities are discovered on a daily basis. Attackers can take advantage of these avenues to launch malicious attacks against GCFB. Scans and penetration tests help find these problem areas proactively so they can be blocked. The difference between scans and penetration tests is that scans are performed using automated tools of GCFB's Internet Protocol (IP) addresses and report on vulnerabilities, rating them by level of criticality. Penetration tests are performed by trained individuals who are granted explicit permission by GCFB to actively try to penetrate systems and applications as if they are an attacker.

Reference: Testing and Scanning Policy.

7.26 THIRD-PARTY ACCESS AND MANAGEMENT

Threats can be introduced to GCFB's environment simply by connecting a third-party without efficient security practices and controls in place. Should an attacker penetrate the third-party's network, they may route their way via the connected third-party into GCFB's network. In some cases, third-parties have privileged access (meaning they have direct access to cardholder data in the production environment), thus gaining unauthorized access to the cardholder data environment.

Should an unauthorized user obtain access to GCFB's network via this route, they may do so under the pretense of being the third-party and therefore potentially penetrate systems, applications, and other networks unnoticed to gain additional access to sensitive data. This can lead to a security breach, causing harm to GCFB's finances, operations, and brand name.

A third-party, in Payment Card Industry (PCI) terms, may either transmit, process, and/or store cardholder data on behalf of GCFB, but also may be connected to perform non PCI-related functions. Therefore, it is important to safeguard GCFB from attackers masquerading as an authorized third-party, as well as proactively validating the security controls and practices in place at connected third-parties.

There are several types of third-parties, the most common being resellers, point of sale (POS) providers, Information Technology support companies, software application developers and vendors, shopping cart vendors, off-site storage vendors, data center and Web hosting providers, and Service Providers (those companies which transmit, process, and store cardholder data on GCFB's behalf. GCFB maintains primary relationships with <types> for the purpose/s of <purpose>.

Reference: Third-Party Access and Management Policy.

An accurate clock which synchronizes time across systems is critical to safeguard GCFB's cardholder data environment as identical timestamps support systems and applications transmitting, processing, and/or storing this sensitive data.

Identical system timestamps support the effectiveness and accuracy of several processes and technologies, to include services set to run at a specific time, log management and analysis,

forensic investigations, server requests, commands, and more. It is common for system components to have their time begin to lag or change over an extended period of time. Subsequently, all system components need to maintain identical timestamps. A clock synchronization system needs to be implemented across all systems-in-scope, with a dedicated server or servers pulling the time from an established external time source. Those servers, in turn, distribute the time to the other systems.

Reference: Time Synchronization Policy.

SECURITY AWARENESS GUIDE ACKNOWLEDGEMENT & RECEIPT

I acknowledge that I have received and understand the Security Awareness Guide and policies reviewed throughout this document.

I acknowledge that all of my questions or clarifications requested in regards to these policies and procedures have been answered and reviewed to my satisfaction.

I understand that it is my responsibility to read and comply with each policy within the Security Awareness Guide and any revisions made to it. I understand that failure to adhere to these Company policies and procedures may result in disciplinary action, up to and including termination of employment or criminal prosecution where laws have been broken.

_____ _____

Employee's Signature Date

_____

Employee's Name (Print)

TO BE PLACED IN EMPLOYEE'S PERSONNEL FILE