2026 Security Awareness

Company Policies and Processes

For OCEDON Restaurants with operations at
9635 Maroon Circle, Suite 300, Englewood, CO 80112

Issued on 01/01/2019
Updated on 01/01/2026

Prepared By

Brian M. McMillen
Information Technology and Loss Prevention Manager
OCEDON
A Burger King Franchise Group
C: 740.815.6207
brian@ocedon.com
Apply online! www.ILuvBK.com

Table of Contents

Company Policies and Processes Overview

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, the Company Brand, the Enterprise Network, Cardholder Data and Sensitive Authentication Data. The policies in this guideline 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 to the Organization

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

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 the upper management. Management will make every effort to correct this situation and expects to be notified if credit card information is ever exposed.

NOTICE: If you can see more than the last four digits of the sixteen-digit Credit Card Number, report this situation to management

Our Company 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. Track 1 is 79 characters in length, is alphanumeric and contains the account number, the cardholder's name, and the additional data listed on Track 2. 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)
3. 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 for Employees 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. In the event that information must be written down due to a business exception, as soon as the credit card authorization has been approved and the transaction has been verified complete the information must be destroyed per company policy (and paper must be crosscut shredded to the size of ¼").

   NOTICE: This is never to be done without written authorization and signed by the Technology Manager.
5. 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.
6. Do not write down Cardholder or Sensitive Authentication Data in guest books, catering logs or future event orders.
7. Do not post future event orders with Cardholder or Sensitive Authentication Data in public locations. They must be locked in a secure location at all times.
8. 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. Example: Mr. / Ms. Smith thank you for visiting our restaurant today we appreciate your business.
9. 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 via crosscut shredding to the size of ¼". If the guest returns or calls after 24 hours, notify them that the card was destroyed to protect their account security.'

   NOTICE: Notify management immediately if a customer leaves their credit card behind.

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 go through offline mode within the Point-of-Sale system. Offline mode will allow you to continue to accept credit cards into the system and they should automatically process when the credit card processing comes back online.

> **NOTICE:** At no time does Ocedon authorize any person to physically write down customer credit card data without written and signed consent from the Technology Manager. If the Point-of-Sale refuses online or offline transactions, then credit card processing will not take place at the location until the issue has been rectified by the Technology Manager or Point-of-Sale vendor.

If both the Point-of-Sale and credit card processing are not functioning, the crash kit process must be implemented. Ask management to call the Technology Manager or Point-of-Sale vendor to rectify the problem. Ocedon does not allow a manual card imprinter, commonly known as a knuckle buster, and credit card slips.

Once the systems are back online the credit card information will automatically process in the Point-of-Sale system.

3 Security Fraud Awareness (Cyber Crime)

While our company 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 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 are commonly affected by malware that have access to sensitive cardholder data must be running anti-malware software that can detect and eliminate known forms of malware. At least once per year, management will verify that systems that were previously considered to be unaffected by malware still fall into that category. If for whatever reason, the malware protection on a system must be temporarily disabled, it must be deactivated by authorized personnel with management's approval. As soon as possible, the anti-malware must be reactivated.

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 the Technology Manager and report suspicious behavior on the computer systems to Ocedon Senior Leadership and Technology Manager.
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 the Technology Manager.

3.2 Email

3.2.1 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.

3.2.2 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.

NOTICE: If you suspect that you are receiving spoofed messages contact management

3.2.3 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

3.2.4 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.

3.2.5 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 not to send them in the future due to the company's inability to guarantee that such data would be protected.

Ocedon Senior Leadership 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 an additional web browser, upgrade the existing web browser, or replace the existing corporate approved web browser.

NOTE: For example, the Mozilla Firefox 2.0 browser's password manager can reveal your passwords in clear text.

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

CAUTION: 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.

3.4.1 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. Other devices can be attached to the payment terminal and intercept credit cards during the transaction. These numbers are then sold to cyber-crime rings. It is your responsibility to report any suspicious activity to management.

Periodically, it will be management's responsibility to physically examine any device which is legitimately used in the credit card transaction process for signs of tampering to try and identify if a skimmer or related piece of hardware has been added to the payment environment. If such a device is discovered escalate the incident to either management or law enforcement as appropriate.

3.4.2 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.

NOTICE: At no time shall any person employed by Ocedon manually write down credit card information for current or later use.

3.4.3 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. Do not be fooled if someone contacts you and requests sensitive information. You should always contact management for approval. 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.

3.5 Passwords

This policy applies to any and all personnel who have any form of user or administrator account requiring a password on any Company network, system, or system component.

Passwords must be protected at all times per the User ID Management and Password Policy described below.

3.5.1 User ID Management and Password Policy

The Company shall assign a unique identification (ID) to each person with access to any Company network, system, or system component to ensure that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. The Company shall perform user ID management in accordance with the following standards:

1. All users shall be identified with a unique username before allowing them to access system components or cardholder data. Terminals used for orders but without access to stored credit card data are not included in this policy.
2. In no event shall group, shared, or generic accounts and passwords be assigned for any network, system, system component, application, data access, or any other information resource.
3. In addition to assigning a unique ID, the Company shall employ at least one of the following methods to authenticate all users:
   - Password
   - Token devices (e.g., SecureID, certificates, or public key)
   - One Time Passwords (two-factor authentication)
   - Biometrics
4. The Company shall use two-factor authentication for remote access to the network by employees, administrators, and third parties. The second factor will have the feature such that a compromise of credentials alone will be insufficient to allow for remote access.
5. Why should you protect your password? Our organization has implemented security procedures that allow for the forensic investigation of all activity that occurs in the company's system environment. In the event of fraudulent activity such as a credit card breach, we will track activity back to the user logged into the system at the time of any event. To ensure that you are not incorrectly accused of improper activity due to the behavior of others, never share your password with anyone. The Company shall develop systems that will transmit passwords only utilizing strong cryptography as they transverse the network. It is specifically prohibited for employees to bypass this security measure. If you feel that your password has somehow been compromised, make sure that it is changed immediately.
6. Following certain basic policy rules regarding the safekeeping and non-dissemination of password information will prevent the large majority of inadvertent exposure of passwords. These rules include:
   - Never write passwords down.
   - Never send a password through company email.
   - Never include a password in a non-encrypted stored document.
   - Never tell anyone your password.
   - Never reveal your password over the telephone.
   - Never hint at the format of your password.
   - Never reveal or hint at your password on a form on the internet.
   - Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
   - If anyone asks for your password, refuse and discuss the situation with Ocedon Senior Leadership or Technology Manager.
   - Be careful about letting someone see you type your password.
7. Change your password at least every 90 days. A password or pass phrase is a secret code that allows you, and only you, to access company systems. Changing your password on a regular basis helps to prevent unauthorized access to your account.
8. If you do not know how to change your password notify your Technology Manager and have them review the step-by-step process.
9. How to choose a strong password that meets the security requirements of the company:

   - Minimum Length - 8 characters
   - Maximum Length – 10 characters
   - Use a combination of lowercase letters, uppercase letters, numbers and special characters (@#$%^&*(){}[]!)
   - Avoid common patterns – dictionary words, common acronyms, reverse spelling of words, names of people or places, part of your login name, or parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses
   - Password history – a minimum of four unique passwords before an old password may be reused

10. Password protected screen savers should be enabled and should protect the company computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. As an alternative to password protected screen savers, users may lock their computers. This leaves the computer functioning, but it cannot be used until someone with a password unlocks it.

3.5.2 User Authentication and Password Administration

The Company shall ensure proper user authentication and password management for non-consumer users and administrators on all systems and system components as follows:

1. Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
2. Verify user identity before performing password resets.
3. Set first-time passwords to a unique value for each user and change immediately after the first use.
4. Immediately revoke access for any terminated users.
5. Remove inactive user accounts at least every 90 days.
6. Enable accounts used by vendors for remote maintenance only during the time period needed.
7. Communicate password procedures and policies to all users who have access to cardholder data.
8. Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
9. Limit repeated access attempts by locking out the user ID after not more than six attempts.
10. Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
11. If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
12. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.
13. Verify that application ID's are only able to be used by the applications (and not by individual users or other processes). This is often ensured by limiting access to internal ID's that are used for the application and best practice is to make sure that no one in the company has access to such ID's.

3.6 Key Management

This policy applies to the use, implementation, storage, destruction, replacement, and revocation of cryptography keys which are crucial to protecting cardholder data.

Cryptography keys must be protected so that the decryption of cardholder data is not practical whenever the data is stored.

3.6.1 Successful Key Management

The Company relies upon 3rd party POS professionals to install and maintain the keys necessary to encrypt the cardholder data in use by the POS system.

1. The keys are implemented at the installation of the POS software
2. Do not retain, write down, or otherwise hold the keys in any company system.
3. Only the 3rd party POS resources used to maintain the POS system will have access to any key data.
4. If keys must be added, replaced, re-injected, or otherwise managed after the initial installation, the company will only utilize the trusted 3rd party POS resources to manage the process.

3.6.2 Daily Log Review and Alerts

The company expects that daily log review will occur in the following manner for each system involved with credit card transactions.

1. Security devices such as firewalls will be examined by Netsurion using automated alert generations and engineering review.
2. Rogue Device Alerts (if any are generated) as sent by Netsurion must be investigated to determine if something has been added to the Point-of-Sale environment inappropriately or if a new baseline must be monitored by Netsurion. They must not be ignored.
3. For any system that stores credit card data, a daily review of critical events must occur, and any event determined to pose a risk to the credit card environment must be escalated as defined in the Incident Response Policy that follows.

4 Incident Response Policy

4.1 Response Plan

The following steps will be taken during an incident (suspected illegal use of a corporate system) or a security breach (an incident that results in the loss of sensitive data). It is important that you follow the company guidelines in the event of a data compromise. You may be asked to sign off on the final incident report or make a statement as to what you have observed.

1. The person who discovers the incident will call management who should know how to contact other resources (as described below) Management will determine which (if any resources are needed):

   - IT / POS support
   - Intrusion detection monitoring personnel
   - A system administrator
   - A firewall administrator
   - The business partner who will represent the interest of the company
   - The company's legal representative (determine state notification obligations under the law and contractually)

2. Management should log the following information about a reported incident:

   - The name of the person who realized that there may be an issue
   - The time it was discovered
   - The time of the first notification
   - The nature of the incident (short description)
   - The equipment (access point, server, pos terminal, etc.) or persons (name and shift) involved
   - Location of equipment or persons involved
   - How the incident was detected?

3. Management will need to identify:

- Is the equipment affected or person involved business critical?
- What is the severity of the potential impact?
- Affected system details (name of computer, operating system, IP address, location)
- Information about the attack (IP address of attacker, name of software used, pictures of where a key logger was found, etc.)

4. Management, potentially with the help of those called for support, will need to determine:

- Is the incident real or perceived?
- Is the incident still in progress?
- What data or property is threatened and how critical is it?
- What is the impact on the business should the attack succeed? Minimal, serious, or critical?
- Is the incident inside the trusted network?
- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker, and should that affect the response or remediation?
- What type of incident is this? Ex: virus, worm, intrusion, abuse, damage.

5. Management, potentially with the help of those called for support, will write a report detailing the incident:

- List the severity of the incident
- Categorize the type of incident (worm, virus, system failure, unauthorized intrusion, system abuse, employee activity, file integrity monitoring alert, log indication of unauthorized activity, etc.)
- Result of the incident (data loss – breach, contained without data loss, undetermined if data was lost, investigation determined no threat to data, etc.)

6. Management will determine if it is necessary to record information for further forensic investigation if the incident response determines that a loss of sensitive data is possible. The techniques management will employ to facilitate this process include:

- Reviewing system logs (and looking for gaps)
- Interviewing witnesses and the incident victim to determine how the incident was caused
- Capturing system images and having the data examined to look for the signs of unauthorized activity, access, or applications

7. Management, potentially with the help of those called for support, will restore the affected system(s) to an acceptable state. They may do any or more of the following:

- Evidence Preservation – Management will keep copies of logs, email, and other documentable communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

- Notify proper external agencies - Notify the police and other appropriate agencies if prosecution of the intruder is possible. If a breach is identified, notifications to the credit card brands may be required. Contact merchant bank (or acquiring bank) after a breach is confirmed as to the need to further report the incident to the card brands. Determine with legal counsel if government or public notification is required under the law.

- Review response and update policies - Plan and take preventative steps so the intrusion can't happen again.

4.2 Response Preparedness

The Company shall test the Response Plan at least once annually to the degree and extent that it is appropriate for its operations. The test may include but is not limited to the following:

- Do employees know how to report an incident?
- Does management know what information to log?
- Does management know how to assess the incident?
- Does management know how to notify the appropriate parties?

5 Facility Access Control Policy

The Company shall use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.

5.1 Monitor Sensitive Areas

The company shall ensure that video cameras or an approved company method of tracking individual physical access are used to monitor sensitive areas where payment card information is stored. The collected data from camera monitoring shall be audited and correlated with other entries. Video data shall be stored for at least three months, unless otherwise restricted by law. All managers' offices and desks with sensitive information or systems will remain secure and locked unless occupied. It is your responsibility to notify management immediately if a secure area is noticed to be unlocked.

5.2 Physical Access Restriction

The company shall ensure that physical access to publicly accessible network jacks, wireless access points, gateways, and handheld devices are restricted to Company or contractor personnel on a need to access basis. It is your responsibility to greet any unauthorized personnel that you may see in restricted areas, confirm that they are authorized to be present and ask them to leave the secure area until you receive confirmation. In the event that an intruder does not wish to leave do not confront them directly. Notify management of their presence and contact the police via 911 for assistance in removing them from the area if appropriate.

NOTICE: It is your responsibility to greet any unauthorized personnel that you may see in restricted areas, confirm that they are authorized to be present and ask them to leave the secure area until you receive confirmation.

5.3 Visitor Access Control

The company shall develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are resident on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

6 Acceptable Use Policy

6.1 Overview and Purpose

The Company's intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the Company's established culture of openness, trust and integrity. The Company 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 the

Company. 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 the Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.

6.2 General Use and Ownership

While the Company 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 the Company. 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 the Company.

The Company, in its routine management of the business, shall conduct the following IT oversight activities:

1. For security and network maintenance purposes, authorized individuals within the Company may monitor equipment, systems and network traffic at any time.
2. The company 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 the Company network that has access to cardholder data, must be inventoried and approved by Company management.

6.3 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 the Company. 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, the Company 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.

6.4 Protection of Proprietary and Sensitive Data, including 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 the Company network. Furthermore, only systems that are specifically authorized on the Company's list of approved software and hardware are eligible for connection to the Company'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.

NOTICE: 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 the Company network must be encrypted with WPA or WPA2 encryption. Wireless access to the Company 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 the Company to install critical security patches within 30 days of their release.

NOTICE: 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.

7 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 the Company 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.

7.1 Unacceptable System and 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 the Company.
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 the Company 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 Company Name account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless specifically requested by management.
11. 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.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. 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.
15. Providing information about, or lists of, Company employees to parties outside the Company.
16. Writing down sensitive information such as Cardholder or Sensitive Authorization Data and removing from Company premises or using for personal gain.

8 Data Retention and Storage Policy

The Company’s Data Retention and Storage Policy provides a risk mitigation opportunity since one method for minimizing risk includes not storing cardholder data unless absolutely necessary.

8.1 Minimize Storage and Retention of Cardholder Data

The Company shall keep cardholder data storage to the minimum necessary to conduct business operations, and cardholder data shall only be retained for that amount of time which is required for business, legal, and/or regulatory purposes.

At no time shall any cardholder data be stored in any form outside of approved Company systems. The following storage mechanisms for cardholder information are prohibited:

1. Hardcopy, including guest books, paper notes, notebooks, receipts, or any other hardcopy format
2. Personal computers, including laptops or other PC’s, whether personally owned or Company resources

3. Electronic storage devices, including portable USB flash drives, other flash memory, magnetic storage media, and any other form of electronic storage (except tape or other mass storage used for back-up purposes at Company or host provider sites).

8.2 Storage and Control of Media

The Company shall ensure that any media that contains cardholder data is managed and controlled as follows:

1. Media back-ups shall be stored in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility
2. The Company shall maintain strict control over the internal or external distribution of any kind of media that contains cardholder data with the following actions:
    a. Classify the media so it can be identified as confidential
    b. Send the media by secured courier or other delivery method that can be accurately tracked
    c. Management shall specifically approve any and all media that is moved from a secured area (especially when media is distributed to individuals).
3. The Company shall maintain strict control over the storage and accessibility of media that contains cardholder data. As appropriate, management will verify at least quarterly that cardholder data is not being stored in violation to these policies and procedures. The company shall also confirm that containers holding cardholder data are secured themselves (such as the container used to hold paper waiting to be shredded).
4. All media shall be inventoried on an annual basis.

8.3 Storage and Control of Hardcopy

Although hardcopy of cardholder data (e.g., guest books, paper notes, notebooks, receipts) is prohibited by the Company as cited above, should hardcopy cardholder data be discovered, then the user or administrator who discovers the hardcopy data is responsible for ensuring that it is physically secure until disposition can be properly determined.

8.4 Destruction of Cardholder Data

Any cardholder data that has been found to be stored on any of the mechanisms shall be destroyed through secure methods described herein, with the exception that if the mechanism must be preserved for forensic investigation or other legal or regulatory matter, then the mechanism shall be isolated and stored securely. Programmatically, cardholder data will be eliminated from any relevant database at least quarterly.

8.5 Destruction of Electronic Cardholder Data

The Company shall destroy any electronic cardholder data by electronically formatting the media or pulverizing it so that it is unrecoverable by commercially available means.

8.6 Prohibited Data Storage

The Company shall not store sensitive authentication data subsequent to authorization in any form, encrypted or unencrypted.   Sensitive authentication data includes the following data:

1. The full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.
2. The card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions

3. Do not store the personal identification number (PIN) or the encrypted PIN block.

9 Visitor Log

9.1 Usage - to track access to sensitive areas of the business

9.1.1 Print copies of this page as needed

9.1.2 Retain each page of the log for at least 30 days

Name of Visitor	Visitor's Firm	Date	Employee who allowed access

10 Hardware Inventory of Payment Devices

10.1 Usage - to record devices involved with credit card transactions. Inspect devices at least once per year.

10.1.1 Print a new copy of this page for each periodic inspection

10.1.2 Update this list whenever there is a move, add, change or removal of a device.

10.1.3 Store number / Address:____

Make / Model of Device (	Serial Number / Asset Tag	Date
Verifone P400 – Terminal 0		
Verifone P400 – Terminal 1		
Verifone P400 – Terminal 2		
Verifone P400 – Terminal 10		
Verifone P400 – Terminal 11		
Verifone P400 – Kiosk 1		
Verifone P400 – Kiosk 2		
Verifone P400 – Kiosk 3		

11 Acknowledgement of Receipt of Security Awareness Policies and Processes

I ________________________________ on this day __________________ acknowledge that I have received and understand the Security Awareness Policies and Processes reviewed throughout this document.

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

I understand that failure to adhere to these company policies and programs may result in disciplinary action, up to and including termination of employment or criminal prosecution where laws have been broken.

Comments: ____

Name/Location: **BURGER KING**	Location Identifier (Number): **#**
Restaurant Manager Name (printed or typed):	Senior Leadership Name (printed or typed):
Restaurant Manager Signature:	Senior Leadership Signature:
Date:	Date:
Used for IT or Human Resources Only:	
Name of IT or HR Resource Receiving File:	Date of Verification of Review and entry into company employee files:
Assistant Manager Name:	Assistant Manager Signature:
Assistant Manager Name:	Assistant Manager Signature:
Assistant Manager Name:	Assistant Manager Signature:
Assistant Manager Name:	Assistant Manager Signature:
Assistant Manager Name:	Assistant Manager Signature:
Assistant Manager Name:	Assistant Manager Signature:

12 Revision History

Changes	Approving Manager	Date	Version
Initial Publication	**Reviewer Name**	**DD-MM-YYYY**	**1.0**
January 2019	Brian McMillen	01-01-2019	1.0
January 2020	Brian McMillen	01-01-2020	1.0
January 2021	Brian McMillen	01-01-2021	1.0
January 2022	Steve Gonzales	01-01-2022	1.0
January 2023	Steve Gonzales	01-01-2023	1.0
January 2024	Brian McMillen	01-01-2024	1.0
January 2025	Brian McMillen	01-01-2025	1.0
January 2026	Brian McMillen	01-01-2026	1.0