MBR Management Corp
IT Security Policies

This contains confidential information and is intended only for current employees of MBR Management Corp and should not be shared with anyone outside of the organization.

Contents

Access Management Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support/s	Jason Walls	Jeff Tope

Introduction

Without defined access privileges and control, users would be allowed to access systems and applications in MBR Management Corporation'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. MBR Management Corporation'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.

A careful review of each system and application should be performed based on results from risk assessment activities performed by MBR Management Corporation Store Support, 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. A list of active employees can be attained from HR, 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.

Access to critical systems, applications, equipment, and data is required in order for by MBR Management Corporation to maintain business operations; however a user possessing privileges they do not require can lead to an intentional or unintentional security breach, causing harm to by MBR Management Corporation's finances, operations, and brand name.

Purpose

This Access Management Policy details the requirements for the granting, transferring, revoking and management of user access in by MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at by MBR Management Corporation, whether conducting activities on by MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by by MBR Management Corporation whether located on by MBR Management Corporation premise or off-site, and all by MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at by MBR Management Corporation, to include by MBR Management

Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com. or online at www.mbrdominos.com.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the by MBR Management Corporation Director of Store Support for review and approval using an email.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Access Privileges

Users are to be assigned access privileges based upon the individual's business role and function, following the practice of business need-to-know and right-to-know. A structure of role based access control should be established so that specific functions receive standardized levels of access. Once assigned, the access granted should be reviewed to ensure that it is the lowest level necessary for the user to perform their job requirements. All store employees will be granted Front line access, which is the least access available. As they get promoted they will be granted more access as needed. The access levels in a store are based on position.

Acknowledgement of Access

Users are to receive MBR Management Corporation's information security policy and sign their acknowledgement of following by MBR Management Corporation's requirements prior to gaining access.

Tracking

All access granted, transferred, or revoked is to be tracked in email, and signed by the user's manager and the system owner prior to being granted. This form should include the user's name, location, department, date of access action taken, model after existing user (if applicable), and the access granted.

Review

Access privileges are to be reviewed on a quarterly basis by the user's manager.

Inactive or Disabled Accounts

Access accounts found to be inactive or not appropriately assigned are to be disabled/revoked and removed within 90 days.

Granting Access

All store employees will be granted Front line access, which is the least access available when their employee profile is pushed to a store. An email must be sent to jwalls@mbrmgt.com to grant VPN access.

If anyone needs access to the network cabinet, you must notify Store Support using the online form located on www.mbrdominos.com/IT or scan the QR code using your phone and open the link. DO NOT Share any sensitive data on this form. Report anyone that arrives to perform work. Please provide their name, company, date, and time of visit and what they are providing service on. This should include anyone doing maintenance on equipment, utility companies, property management, etc.

Report all unexpected visitors, suspicious items or someone tampering with equipment immediately. Anyone that is requesting access behind the counter and is not expected must be verified **BEFORE** being allowed behind the counter. You should get the person's information and contact your supervisor for further instructions. If your supervisor is not available call Store support at 636-947-4433 x2513. Any suspicious items (USB drives, strange cables, things attached to the cc readers) should be removed and stored in a safe place, stop using the affected equipment, unplug it from the network and power and report immediately.

If anyone is seen tampering with computers or network equipment, they must be stopped immediately and reported to store support.

Changing Access

An email to Store Support is used to approve the access prior to it being changed.

Removing Access

An email to Store Support must be sent If the user has been terminated from the company, the user's manager must notify the MBR Management Corporation HR Manager and Store support to disable/revoke the user's access immediately, should the termination be unfriendly. If the user holds privileged access to PCI systems or data, their access ID should be removed unless it is absolutely critical for business operations. An email must be sent to revoke VPN access.

Privileged Users

Individuals with privileged IDs, such as security administrators, are to have separate accounts for their user-level activities and for their privileged functions. The user may not use their privileged ID for general user activities.

Anti-Virus Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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

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 by MBR Management Corporation, customers, and third-parties. Anti-virus software can help protect by MBR Management Corporation systems from being affected by attacks and help safeguard by MBR Management Corporation's finances, operations, and brand name.

Purpose

This Anti-Virus Policy details the requirements for the deployment, configuration, and management of anti-virus software in by MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at by MBR Management Corporation, whether conducting activities on by MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by by MBR Management Corporation whether located on by MBR Management Corporation premise or off-site, and all by MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at by MBR Management Corporation, to include by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the by MBR Management Corporation Director of Store Support for review and approval using an email.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Deployment

Anti-virus software must be deployed on all servers, workstations, and gateways which are considered to be those commonly affected by viruses. The anti-virus software should be an up to date/current enough version that it protects against spyware and adware. The anti-virus software will be managed by DPZ

Configuration

Configuration of the software must follow the vendor-provided guidance and standards, with exceptions reviewed and approved by the MBR Management Corp. Store Support. The software should be configured so that users cannot disable or tamper with it.

Scanning

Anti-virus software should be set to scan in “auto-protect” mode to automatically scan new files in creation, incoming and outgoing email attachments, and downloaded files. A full workstation scan should be set to be performed at a minimum, weekly, and a full server scan at a minimum, daily.

Lab Testing

If a scan is set to occur during lab testing, the anti-virus should take precedence and be run first. If the software needs to be disabled, it must be enabled again once the testing is complete.

Logging

Anti-virus event logs are to be generated and retained for at least 365 days. These logs should contain dates of scans performed and incidents found.

User Responsibilities

All users are to be aware/trained on how to prevent, detect, and respond to an incident which may be related to a virus, specifically users should know not to click on an attachment from an unknown person or if their system is running slow or acting up. Users are to report suspected incidents to Store Support.

Backup Tape Security Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

Backups are made for systems transmitting, processing, and/or storing sensitive data in order to be able to reinstitute data and configurations should the system become compromised or in the event of a disaster. by MBR Management Corporation'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.

Purpose

This Backup Tape Security Policy details the requirements for the safeguarding of backup media containing cardholder data in by MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at by MBR Management Corporation, whether conducting activities on by MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by by MBR Management Corporation whether located on by MBR Management Corporation premise or off-site, and all by MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at by MBR Management Corporation, to include by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the by MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Cardholder Data Storage

Cardholder data must not be stored. Therefore, should backups be made of systems transmitting and processing this data, careful reviews should be made on a periodic basis to determine if cardholder data is being stored on the media.

Handling

Backup media are to be treated according to the Mission Critical data labeling, handling, retention, and disposal policies. Backup media may be reused as long as the content is deleted per by MBR Management Corporation disposal policy.

Third-Party or Alternate Location Storage

If backup media(s) containing cardholder data are retained by a third-party location, they are to be tracked and protected against loss of theft. A certified and insured third-party must be used to handle the cardholder data at all times. The media must be counted and tracked at the point of departure and also at the point of arrival, in the case of inconsistencies, Store Support will be notified in due time. A PCI-compliant service provider is recommended when using a third-party storage facility.

Tracking Logs

A log is to be maintained of the transports with by MBR Management Corporation Management signature. Transport logs are to be retained for a minimum of 365 days. The media must be counted and tracked at the point of departure and also at the point of arrival, in the case of inconsistencies, Store Support will be notified in due time.

Secure Configuration Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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. by MBR Management Corporation'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.

Each system and networking component should be included in the annual risk assessment performed by by MBR Management Corporation Store Support 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.

Deviations from secure configurations can lead to an intentional or unintentional security breach, causing harm to by MBR Management Corporation's finances, operations, and brand name.

Purpose

This Secure Configuration Policy details the requirements for the safe configuration of systems and networking equipment in by MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at by MBR Management Corporation, whether conducting activities on by MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by by MBR Management Corporation whether located on by MBR Management Corporation premises or off-site, and all by MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at by MBR Management Corporation, to include by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members. The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the by MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Documentation

Secure configuration standards are to be documented for each system and networking component in the cardholder environment. These documents are to be based on accepted best security configuration practices (to include those from SANS, CIS, ISO) or vendor guidelines (Microsoft, Apache, Oracle) or a combination of both. Should the guidance not be applicable in by MBR Management Corporation's environment or it has been decided to be excluded from by MBR Management Corporation's secure configuration standards, an exception is required to be created and approved by by MBR Management Corporation Store Support by MBR Management Corporation secure configuration standards must be updated whenever there is a change made to the environment, a change made to the system or networking component, or an exception is made.

Basic Requirements

The following are required to be included in by MBR Management Corporation's system configuration documentation, at a minimum:

- Inventory of systems and networking equipment, along with their name, purpose, location, date of deployment, and owner.
- Servers may only perform one function each if they are used in the cardholder environment.
- Services and applications, if not in use, are to be disabled.
- All insecure services, applications, and protocols must be reviewed and assessed for their risk. by MBR Management Corporation Store Support must review and sign their acceptance of the risk. An exception request, to include their business justification, must be retained for the lifetime of the exception.
- All firewall ports should be restricted to only those required for the environment. Requests to open up a port or make changes must follow by MBR Management Corporation's firewall policies.
- Default vendor passwords must be changed prior to deployment into production, and then by MBR Management Corporation password policies maintained on the server.
- Patches must be kept current on the servers, and follow by MBR Management Corporation's patch management policies.
- Change control must follow by MBR Management Corporation's change management policies.
- Access permissions must be restricted to business-need only and follow the principle of least privilege.
- Root admin should not be used unless absolutely necessary.
- Access by applications and users must follow by MBR Management Corporation's logging policies.
- Remote access must be two-factor authentication and over secure channels.
- Equipment is to be situated in a secure location protected by by MBR Management Corporation's physical access and equipment protection

Data Classification Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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. by MBR Management Corporation'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.

Printed and electronic data is to be classified in terms of its value to by MBR Management Corporation, 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.

Classifying data can help protect by MBR Management Corporation data from unauthorized access and usage, and help safeguard by MBR Management Corporation's finances, operations, and brand name.

Purpose

This Data Classification Policy details the requirements for the classification of assets and data in by MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at by MBR Management Corporation, whether conducting activities on by MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by by MBR Management Corporation whether located on by MBR Management Corporation premise or off-site, and all by MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at by MBR Management Corporation, to include by MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the by MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Asset and Data Identification

Any asset (system, workstation, removable media, mobile media, backup tape, etc.) and data being processed, transmitted, and/or stored in the cardholder environment is to be identified and documented, along with the asset owner's name, location, and contact information.

Asset and Data Evaluation

A risk assessment exercise should be performed to determine level of risk associated with each asset and data set. The list should be documented and assigned a classification of *High*, *Medium*, or *Low* in terms of its value to by MBR Management Corporation, sensitivity, legal requirements, and impact if lost or misused. Once this is completed, the evaluation should be reviewed and approved by Store Support.

Classification Terminology

Should the asset or data set receive one or more *High* results during the evaluation exercise, it should be labeled as "Mission Critical". If there are no *High* results and the asset or data set carries one or more *Medium* results, it should be labeled as "Essential". If the asset or data set receives no *High* or *Medium* results, it may be labeled as "Normal".

Security Controls

The level of security controls to be in place to safeguard the asset or data set from unauthorized access and misuse will increase with its classification level. For example, a database storing encrypted cardholder data should still be classified as *High* and therefore "Mission Critical", even though the contents are encrypted, as the loss of this data may still cause non-compliance with legal requirements and harm by MBR Management Corporation's reputation. This database would require the highest level of security controls to be in place, to include, but not limited to, being placed behind a firewall and an intrusion detection/prevention system, have restricted access permissions, maintain file integrity software, and have active logging enabled. An asset or data set classified as Normal may be freely released externally and communicated, and may be readily accessible to both internal and external users.

Data Handling

Once the asset or data set have been classified, it is to be transmitted, processed, used, and/or stored following the methods outlined in the Data Handling Policy. An asset or data set without an assigned classification is to be treated as Mission Critical until it is properly classified.

Incident Response

Should a Mission Critical asset or data set be intentionally or unintentionally accessed, viewed, or used by an unauthorized party, the incident response plan is to be initiated. Should it be a Mission Critical asset or data set, Store Support should evaluate the repercussions of the event and initiate the incident response plan as appropriate.

Classification Details

Mission Critical

This type of classification is assigned to assets and data sets which, if lost, would cause serious harm to by MBR Management Corporation, by MBR Management Corporation's customers, by MBR Management Corporation's third-parties, and others. Harmful effects 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.

Essential

This type of classification is assigned to assets and data sets which, if lost, could potentially cause harm to by MBR Management Corporation, by MBR Management Corporation's customers, by MBR Management Corporation'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).

Normal

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 by MBR Management Corporation , by MBR Management Corporation's customers, by MBR Management Corporation's third-parties, and others. Subsequently, it does not require specific security controls.

Examples include by MBR Management Corporation's website, marketing materials, press releases, and external announcements.

Requests for Access to Mission Critical or Essential Assets or Data

The system owner is ultimately responsible for individuals and applications which have access to their assets, and are to review all access requests. The system owner is to review the access permissions on a quarterly basis in tandem with the quarterly access control review exercise.

Awareness

Users are to be trained and made aware of the classifications and their handling requirements. Users who have business requirements to view, access, and use Mission Critical and Essential assets and data are to receive specialized training on how to properly handle those items.

Data Handling Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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. by MBR Management Corporation'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 assets and data according to its classification level can help protect by MBR Management Corporation data from unauthorized access and usage, and help safeguard by MBR Management Corporation's finances, operations, and brand name.

Purpose

This Data Handling Policy details the requirements for the transmission, storing, and usage of assets and data in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Cardholder Data

Cardholder data may never be transmitted using any end-user methodologies unless specifically approved by Store Support with a valid business need. If required to transmit cardholder data, it must be in unreadable format (for example, encrypted, masked, truncated). Users may also not store cardholder data without specific approval to do so from Store Support at which point it must also be retained in a protected format. The only exception is for users who need to view cardholder numbers for business reasons, these users must be approved by Store Support and may only view the number individually (meaning one by one).

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

Access:	Business need-to-know only. Reviewed quarterly.
Non-Disclosure (NDA):	MBR Management Corporation third-parties and employees may only access these assets and data after signing an NDA. The system owner must then approve the distribution.
Changes:	Changes made to these assets and data sets must be approved by Store Support and the system owner prior to the change, recorded and retained for minimum of one year.
Email:	Only individuals approved by Store Support to transmit this data may do so, and then only if the email and its attachments are approved using a MBR Management Corporation -approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non- MBR Management Corporation 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 MBR Management Corporation 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 which 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 Store Support. 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 MBR Management Corporation -approved method. This includes data storage on workstations, systems, backup tapes, etc.

Handling Requirements for Assets and Data Sets Labeled as Essential:

Access:	Business need-to-know only. Reviewed quarterly.
Non-Disclosure (NDA):	MBR Management Corporation third-parties and employees may only access these assets and data after signing a NDA.
Changes:	Changes made to these assets and data sets must follows the MBR Management Corporation Change Management Policy.
Email:	Only individuals approved by Store Support to transmit this data may do so, and then only if the email and its attachments are approved using a MBR Management Corporation -approved encryption method. A receipt request should be used or requested.
Internet:	This data may never be transmitted using a non MBR Management Corporation 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 MBR Management Corporation 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 which 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 Store Support. 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 MBR Management Corporation -approved method. This includes data storage on workstations, systems, backup tapes, etc.

Handling Requirements for Assets and Data Sets Labeled as Normal:

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 MBR Management Corporation'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 MBR Management Corporation
Printing:	May be readily printed
Print Storage:	Does not need to be stored securely
Electronic Storage:	Does not need to be stored securely

Data Retention Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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. MBR Management Corporation's cardholder environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage phase(s) of cardholder data.

Each asset and data set (both electronic and printed formats) should be reviewed by a Legal point-of-contact to assess MBR Management Corporation'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.

The retention of assets and data for the minimum length of time possible under law and to support business operations can help protect MBR Management Corporation data from unauthorized access and usage, and help safeguard MBR Management Corporation's finances, operations, and brand name.

Purpose

This Data Retention Policy details the requirements for the retention of assets and data in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Retention of Cardholder Data

Cardholder data should only be retained for the minimum length of time as is possible, once legal, industry, financial, and regulatory requirements are reviewed and applied. Representatives from the Legal and Management groups, as well as the system owner, should assess these requirements and define the retention period for each asset and data set, following the guiding principle that the item should be retained for the least amount of time as is possible.

The form in *Appendix A* of this Policy must be completed for each data set being retained.

Retention of Sensitive Authentication Data

Sensitive Authentication Data (the magnetic strip, PIN blocks, CVV) may never be stored after authorization, unless there is a specific business need to retain this data. The PCI Data Security Standards have specific requirements for what comprises a business need for the retention of this data, and the MBR Management Corporation's bank or a cardholder brand should be consulted prior to storing this data. The Sensitive Authentication data may be retained prior to authorization, but must be safeguarded following the requirements outlined for "Mission Critical" data in the Data Handling Policy.

Retention Periods

Data is to be deleted, at a minimum, quarterly or preferably more frequently, unless defined during the assessment exercise that it is required to be retained for a longer period of time. If it must be retained for longer than 90 days, a review should be performed quarterly to ensure that the data has not been retained past its defined storage period.

Responsibilities

The system owner or the data owner is ultimately responsible for ensuring that assets and data sets under their ownership are not retained past the defined periods. Store Support is responsible for performing the physical destruction or deletion of data.

Third-Parties

Third-parties must receive a copy of MBR Management Corporation's data labeling, handling, retention, and disposal policies and follow them exactly. Periodic, unannounced reviews should be made by MBR Management Corporation to ensure that the third-party does not violate the policies.

Appendix A: Retention Assessment

Data Set or Asset: _____
Purpose/Function: _____
Owner: _____
Assessment Performed by: _____
Assessment Date: _____

Retention Requirements (as applicable):

Legal: _____
Industry: _____
Financial: _____
Regulatory: _____
Other: _____

Data to be deleted on quarterly basis: Yes___ No___
Data to be reviewed on quarterly basis: Yes___ No___

Legal Signature

_____

Management Signature

_____

System/Data Owner Signature

_____

Data Disposal Policy

Version	Date	Change/s	Author/s	Approver/s
2.1	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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. MBR Management Corporation'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.

Secure disposal and deletion methods are required for assets and data sets which are classified as Mission Critical or Essential. Items classified as Normal may be reused freely.

The secure disposal and deletion of assets and data according to its classification level can help protect MBR Management Corporation data from unauthorized access and use, and continue to safeguard MBR Management Corporation's finances, operations, and brand name.

Purpose

This Data Disposal Policy details the requirements for the disposal of assets and deletion of data in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Disposal Requirements for Electronic Data on:

Assets Labeled as Mission Critical

Mission Critical 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 Store Support on a quarterly basis. Users should be made aware of the importance of safely destructing and deleting these assets and data.

If you suspect that card holder data may have been captured on the call recording because the customer started giving information before you were on the payment screen, please report the date time and phone number to store support using the online form located on www.mbrdominos.com/IT immediately so the call can be destroyed.

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 Essential

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

Assets Labeled as Normal

Normal 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 Store Support on a quarterly basis.

Disposal Requirements for Printed Data:

Labeled as Mission Critical

Printed documentation labeled as Mission Critical 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 MBR Management Corporation's terms and conditions of protecting the sensitive data. The destruction schedule should be documented and reviewed by Store Support 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 Essential

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

Assets Labeled as Normal

Normal 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 Store Support on a quarterly basis.

Responsibilities

The system owner or the data owner is ultimately responsible for ensuring that electronic and printed media is disposed of in a secure manner, and the users' managers are responsible for ensuring that their employees follow these policies. Store Support is responsible for performing the actual destruction or deletion of data.

Third-Parties

Third-parties must receive a copy of MBR Management Corporation's data labeling, handling, retention, and disposal policies and follow them. Periodic checks should be made by MBR Management Corporation to ensure that the third-party does not violate the policies.

Critical Technologies Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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 MBR Management Corporation's network in a "non- standard" method, meaning they can be used remotely and not use a MBR Management Corporation workstation in a MBR Management Corporation location. Special care should be made when using these technologies as they are accessing MBR Management Corporation'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. MBR Management Corporation'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.

Properly safeguarding these technologies is critical to help protect MBR Management Corporation from unauthorized users causing harm to MBR Management Corporation's finances, operations, and brand name.

Purpose

This Critical Technologies Policy details the requirements for the usage of remote access, modems, laptops, tablets, and PDAs in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance. The other listed critical technologies are detailed in other MBR Management Corporation Policies.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by MBR Management Corporation whether located on MBR Management Corporation premises or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Remote Access

Remote access into MBR Management Corporation's network must always be comprised of two-factor authentication. This means that there is required to be authentication with something the user knows (password, passphrase) and something the user has (key fob, fingerprint, or individual certificate). These are to be used in conjunction with the user's individual user ID. Remote access must be over a secure, encrypted connection or over a dedicated private line, and logged. Remote access may not be used unless for business purposes, and all users must be approved by Vice President of Finance prior to being granted this access. Only MBR Management Corporation -approved remote access technologies may be used. The session will automatically disconnect after 24 hours and the user will be required to re-authenticate. Third-parties must only be granted remote access permissions and capability after being assessed for risk and approved by the Vice President of Finance, monitored while in use, and then immediately disconnected after use. All users may not copy, move, or store cardholder data using this technology.

Modems

Modems may only be used when required for business operations and require prior authorization from Vice President of Finance. Modems must be labeled with identification information, to include owner, contact information, and purpose. Modems may not be used from any non- MBR Management Corporation location and only MBR Management Corporation -approved modems may be used. Access to the modem itself must be via a unique username and password.

Laptops, Tablets, and PDAs

A list of users granted any of these items is to be kept current by Store Support. Store Support is to be notified of any departing users so their access to MBR Management Corporation's environment may be terminated in a timely manner. Store Support is also responsible for retrieving the equipment back from the departing user. All users are to be approved by their manager prior to being granted the equipment and access to the environment. MBR Management Corporation's access control and password management policies are to apply to the usage of this equipment, and users must be required to authenticate with a unique user ID and password. The device, as feasible, is to be labeled with the owner's name, contact information, and purpose. If this is not possible, a tracking ID number is to be placed on the device, which correlates with the user list maintained by Store Support. These devices may only be utilized for MBR Management Corporation business purposes and must be MBR Management Corporation sanctioned. Users may not use their own devices unless previously authorized to do so by Vice President of Finance. The session will automatically disconnect after 24 Hours and the user will be required to re-authenticate to the device.

Firewall Configuration and Management Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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

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 MBR Management Corporation) and between internal network zones (should one zone contain sensitive systems and the other does not).

Should an unauthorized user obtain access to MBR Management Corporation's network via a route unprotected with a firewall, they may then potentially penetrate systems, applications, and other networks to gain additional access to sensitive data. This can lead to a security breach, causing harm to MBR Management Corporation's finances, operations, and brand name.

Purpose

This Firewall Configuration and Management Policy details the requirements for the configuration, placement, and maintenance of firewalls in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premises or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or non-intentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Placement

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 MBR Management Corporation) and between internal network zones (should one zone contain sensitive systems and the other does not). There may not be direct inbound or outbound access without the placement of a firewall between trusted and untrusted environments.

Environments which are not segmented from the cardholder data environment with firewalls or other form of segmentation (such as a VLAN) must be considered a “flat network” and part of the cardholder environment. All systems, users, equipment etc. within this other environment will be in-scope for PCI assessments.

Network Diagram

A network diagram is to be maintained which accurately depicts the networking equipment, systems, applications, wireless networks, and other applicable components of the cardholder data environment. This includes all inbound and outbound connections, all connected third-parties, locations, security controls in place (i.e.: Intrusion Detection/Prevention Systems), and network segregation in place.

This network diagram must be reviewed and updated after changes are made to the environment, or annually, whichever comes first. The review is to be performed by Store Support and the date of last review documented on the diagram.

Access Rules

Firewalls are to have implicit deny-all rules, unless specific traffic is authorized. Firewall rule sets are to be configured to only permit authorized inbound and outbound traffic by their IP addresses to the trusted environments. Inbound Internet traffic is to be limited to restricted IP addresses <within the Demilitarized Zone (DMZ), should such a zone be in use, or specific systems within the cardholder environment.> Internal outbound traffic from systems within the cardholder environment may only access predefined IP addresses, and admit all inbound and outbound traffic on the MBR Management Corporation network environment to only what is required for business purposes.

Firewall rule sets are to be documented and kept current, and Firewall reviewed by the Director of Store Support on a semi-annual basis, at a minimum. The Director of Store Support must document the review and results in a <firewall review log>. The Vice President of Finance is to review and sign-off on the findings. Exceptions are to be submitted following the Exception process noted earlier in this Policy.

Change Management

Changes may only be made to the configuration of the firewall and the firewall rule sets after a review of the impact of the change has been performed by the Director of Store Support. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from performing the change is to be reviewed and accepted by the Vice President of Finance.

The email to feedback@mbrmgt.com must be used to track changes from their initial request stage though review to documentation of residual risk to approval by Vice President of Finance.

Firewall changes are to be tested in a tested environment prior to being placed into the production environment. Care should be made to carefully monitor deployments of the change once introduced into the production environment when more permissive rules have been introduced.

Traffic Control

Stateful inspection firewalls are to be used, with Network Address Translation (NAT) in place to prevent against IP Masquerading (the broadcast of IP addresses from the internal network to the Internet).

Ports and Services

Only those ports and services which are required for business purposes may be enabled. The firewalls are to explicitly deny inbound and outbound traffic using any other ports and services.

A list of approved ports and services and their business justifications is to be kept current by Director of Store Support and is to be updated after any changed is made. (See Appendix A). Changes are to follow the change management process described earlier in this document.

Protocols

Only those protocols which are required for business purposes may be enabled. The firewalls are to explicitly deny inbound and outbound traffic using any other protocols.

Protocols which are considered “risky” may lead to granting an avenue of attack. Types of “risky” protocols include Telnet, rlogin, and FTP. As any protocol could be considered “risky” if configured incorrectly, care should be made to safeguard against this occurring. These protocols should also not be permitted for use on personal computers with access to the cardholder data environment.

A list of approved protocols and their business justifications is to be kept current by Excel and is to be updated after any changed is made. (See Appendix A). Changes are to follow the change management process described earlier in this document.

Access Controls

Access to the firewall should be limited to only those individuals with a business need-to-know. Individual authentication, meaning a unique user ID and unique password, is to be used by the administrators, unless an Admin account has been specifically approved by Vice President of Finance.

Remote access to the firewalls may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their user ID).

Password management is to follow the password requirements specified in the Password Management Policy.

Event Management and Response

Firewall logs are to be generated, reviewed, and maintained in accordance with the Log Management Policy to provide an audit trail. Logs should include capture of events which have an impact on the configuration of the firewall, unsuccessful attempts to establish a connection via the firewall, packets which are directed to terminate at the firewall, in addition to the requirements presented in the Log Management Policy. Firewall logs should be synced to a central location with logs from the other systems in the cardholder data environment.

Incidents, whether suspected or actual, are to be responded to in accordance with the Incident Response Plan.

Scanning

Firewalls are to be included in the vulnerability scanning initiatives performed by MBR Management Corporation and Control Scan.

Time Synchronization

Network Time Protocol (NTP) or other time synchronization tool is to be used for the firewalls and synced with the other systems in the cardholder environment to maintain consistent times.

Personal Firewalls

Any computers with access to the Internet which are able to access MBR Management Corporation's network are to have a personal firewall enabled and active. This includes computers used by any parties included in the scope of this policy. The personal firewall should be deployed in such a way that it cannot be tampered with and altered by unauthorized individuals.

L**ogical Management of Network Components**

The following individuals are responsible for the logical management of networking equipment:

Configuration and maintenance of firewall rule sets	GLS	Mac@gls.com
Installation of firewalls	GLS	Mac@gls.com
Deployment of firewalls	GLS	Mac@gls.com
Network diagram maintenance	GLS	Mac@gls.com
Reviews of firewall rule set change requests	GLS	Mac@gls.com
Approvals of firewall rule set change requests	GLS	Mac@gls.com

Router Configuration and Management Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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

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.

Should an unauthorized user obtain access to MBR Management Corporation's network they may potentially penetrate systems, applications, and other networks to gain additional access to sensitive data. This can lead to a security breach, causing harm to MBR Management Corporation's finances, operations, and brand name.

Purpose

This Router Configuration and Management Policy details the requirements for the configuration, placement, and maintenance of routers in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members. The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Placement

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 that transmit, process, and/or store cardholder data.

Configuration Services

Routers are to have configuration services defined to support the operating system (OS), as the OS translates the established access control list (ACL) to the router. Configurations are to be configured to permit only authorized inbound and outbound traffic to the trusted environments for only matters required for business purposes.

Router files are to be documented and kept current, and reviewed by the Director of Store Support on a semi-annual basis, at a minimum. The Director of Store Support must document the review and results in a <router review log>. The Vice President of Finance is to review and sign-off on the findings. Exceptions are to be submitted following the *Exceptions* process noted earlier in this Policy.

Change Management

Changes may only be made to the configuration of the router and its configuration files after review of the impact of the change has been performed by the Director of Store Support and DPZ. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from performing said change is to be reviewed and accepted by the Vice President of Finance.

The feedback@mbrmgt.com must be used to track changes from initial request stage through the review of documentation of residual risk to approval by Vice President of Finance.

Router changes are to be tested in a test environment prior to being placed into the production environment. Care should be taken to carefully monitor deployments of the change once introduced into the production environment when more permissive rules have been introduced.

Synchronization of Router Files

Router files are required to be synchronized upon start-up. Changes that are made only to the running configuration won't be retained upon reboot; therefore, changes must be made to the configuration copy in the RAM or to the start-up configuration.

Access Controls

Access to the routers should be limited to only those individuals with a business need-to-know. Individual authentication (a unique userID and unique password) is to be used by the administrators, unless an Admin account has been specifically approved by Vice President of Finance.

Remote access to the routers may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their userID).

Password management is to follow the password requirements specified in the <Password Management Policy>.

Event Management and Response

Router logs are to be generated, reviewed, and maintained in accordance with the <Log Management Policy> to provide an audit trail. Logs should include; capture of events that have an impact on the configuration of the router, packets which are dropped by the router, in addition to, the requirements presented in the <Log Management Policy>. Router logs should be synced to a central location with logs from any other system(s) in the cardholder data environment.

Incidents, whether suspected or actual, are to be responded to in accordance with the <Incident Response Plan>.

Time Synchronization

Network Time Protocol (NTP) or any other time synchronization tool is to be used with the routers and synced with the any other system(s) in the cardholder environment to maintain consistent records of times.

L**ogical Management of Network Components**

The following individuals are responsible for the logical management of networking equipment:

Configuration and maintenance of router files	GLS	Mac@gls.com
Installation of routers	Store Support	Director
Deployment of routers	GLS	Mac@gls.com
Network diagram maintenance	GLS	Mac@gls.com
Reviews of router config file change requests	GLS	Mac@gls.com
Approvals of router config file change requests	GLS	Mac@gls.com

Information Security Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

An Information Security Policy details the acceptable processes and practices for an organization to follow in order to protect the interests of MBR Management Corporation, as well as those of our customers, third-parties, employees, and other entities. This Information Security Policy is required reading for all users who are granted access to MBR Management Corporation's assets upon hire (before being granted access to the assets) and then annually. MBR Management Corporation's assets include anything owned or leased by MBR Management Corporation for operational and business use, to include (but not limited to) systems, data, computers, personal devices, applications, facilities, connections, individuals, documentation, and electronic media, whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

All users are required to always follow this Information Security Policy, unless a prior exception request has been reviewed and approved by a member of MBR Management Corporation Senior Management.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all users granted access to any MBR Management Corporation asset, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Acknowledgement

This policy is to be reviewed and acknowledged via signature by all users granted access to any MBR Management Corporation asset, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members. Signature must be obtained from the user prior to their initial access and then annually as long as the access is maintained.

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Table of Contents

1.0 Why Information Security?

Information Security helps to:

- Safeguard MBR Management Corporation's assets and those belonging to our customers, third-parties, employees, and other entities.
- Support MBR Management Corporation's compliance with regulations, standards, and/or laws.
- Reduce risk to MBR Management Corporation's assets.
- Support the integrity of information and data.

2.0 Usage of MBR Management Corporation Assets

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

The following actions are never permitted when using MBR Management Corporation assets:

- Compromising confidentiality, integrity, and availability of MBR Management Corporation assets.
- Threatening, obscene, profane, offensive language or content.
- Harassing or violating others.
- Gaming, file sharing, music, and other activities.
- Work for another business, commercial venture, or non- MBR Management Corporation - sponsored activities.
- Advertising, purchasing, selling, and transacting non- MBR Management Corporation initiatives.
- Any illegal activities.

3.0 No Expectation of Privacy

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

4.0 Legal and Compliance Requirements

MBR Management Corporation 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.

The following are a sampling of the regulations, standards, and/or laws which MBR Management Corporation 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>
Health Insurance Portability and Accountability Act (**HIPAA):** Protection of Protected Health Information (PHI)>

5.0 Roles and Responsibilities

Users are required to:

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

General Managers are required to:

In addition to the above requirements:

- Ensure that their reports follow MBR Management Corporation policies at all times and understand their roles.

- Designate owners (if not themselves) for MBR Management Corporation assets under their control and management.
- Work with other groups to implement and maintain security controls for assets.
- Participate (as needed and directed) in incident response procedures.

Above Store Managers are required to:

In addition to the above requirements:

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

Store Support is required to:

In addition to the above requirements:

- Oversee and manage compliance with MBR Management Corporation’s policies.
- Perform risk assessments.
- Evaluate and select solutions to reduce risk to MBR Management Corporation assets.
- Write and distribute security policies to all users (as defined in the Introduction).
- Monitor and analyze security alerts and information and distribute to appropriate personnel.
- Define and deploy incident response and escalation procedures.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to data.
- Develop and implement Security Awareness and Training programs.
- Receive alerts from users and other systems 24/7/365.
- 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:

- Champion best security practices from a “top down” approach.
- Take ultimate responsibility for safeguarding MBR Management Corporation’s assets.
- Accept residual risk resulting from assessment initiatives.

6.0 Individual Policies

6.1 Access Control

Without defined access privileges and control, users would be allowed to access systems and applications in MBR Management Corporation’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 MBR Management Corporation, 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 an email to Feedback@mbrmgt.com, 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.

6.2 Anti-Virus

Viruses, and associated spyware, adware, and malware, can infiltrate MBR Management Corporation'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 MBR Management Corporation, customers, and third-parties.

Anti-virus software must be deployed on all servers, workstations, and gateways that are considered to be those commonly affected by viruses. The anti-virus software should be an up to date/current enough version that it protects against spyware and adware.

Reference: Anti-Virus Policy.

6.3 Application Development

As businesses move towards relying on custom-built and off-the-shelf applications to support operations, code vulnerabilities have become one of the most utilized attack vectors to gain unauthorized access to applications transmitting, processing, and/or storing sensitive data.

A Secure Development Lifecycle (SDLC) must be documented, taking into account security considerations and requirements from the inception of the project. A member of the DPZ LLC must be included in the design phase through to deployment. Any code changes to applications, whether internal or external-facing, in the cardholder environment must follow the requirements in the SDLC. The SDLC is to be reviewed and updated whenever there are changes to the application environment, new vulnerabilities discovered, and new secure coding techniques.

Reference: Secure Application Development Policy.

6.4 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 MBR Management Corporation employees. Results from the background checks are to be reviewed and accepted prior to the user being granted access to the environment. Store Support with Human Resources 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.

6.5 Backup Tapes

Backups are made for systems transmitting, processing, and/or storing sensitive data in order to be able to reinstitute data and configurations should the system become compromised or in the event of a disaster.

As backup media may contain cardholder data, it needs to be protected from unauthorized access and/or use just like for any other electronic media containing this content.

Reference: Backup Tapes Policy.

6.6 Change Management

Performing changes to systems and applications in MBR Management Corporation'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.

6.7 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 MBR Management Corporation's network in a "non- standard" method, meaning they can be used remotely and not use a MBR Management Corporation workstation in a MBR Management Corporation location. Special care should be made when using these technologies as they are accessing MBR Management

Corporation'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.

6.8 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 MBR Management Corporation, 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.

Mission Critical

This type of classification is assigned to assets and data sets which, if lost, would cause serious harm to MBR Management Corporation, MBR Management Corporation's customers, MBR Management Corporation's third-parties, and others. Harmful effects 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.

Essential

This type of classification is assigned to assets and data sets which, if lost, could potentially cause harm to MBR Management Corporation, MBR Management Corporation's customers, MBR Management Corporation'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).

Normal

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 MBR Management Corporation, MBR Management Corporation's customers, MBR Management Corporation's third-parties, and others. Subsequently, it does not require specific security controls.

Examples include MBR Management Corporation's website, marketing materials, press releases, and external announcements.

Reference: Data Classification Policy.

6.9 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 Mission Critical or Essential. Items classified as Normal may be reused freely.

Disposal Requirements for Electronic Data on:

Assets Labeled as Mission Critical

Mission Critical 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 Store Support 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 Essential

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

Assets Labeled as Normal

Normal 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 Store Support on a quarterly basis.

Disposal Requirements for Printed Data:

Labeled as Mission Critical

Printed documentation labeled as Mission Critical 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 MBR Management Corporation’s terms and conditions of protecting the sensitive

data. The destruction schedule should be documented and reviewed by Store Support 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 Essential

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

Assets Labeled as Normal

Normal 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 Store Support on a quarterly basis.

Reference: Data Disposal Policy.

6.10 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. MBR Management Corporation'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 Mission Critical:

Access:	Business need-to-know only. Reviewed quarterly.
Non-Disclosure (NDA):	MBR Management Corporation third-parties and employees may only access these assets and data after signing an NDA. The system owner must then approve the distribution.
Changes:	Changes made to these assets and data sets must be approved by Store Support and the system owner prior to the change, recorded and retained for minimum of one year.
Email:	Only individuals approved by Store Support to transmit this data may do so, and then only if the email and its attachments are approved using a MBR Management Corporation -approved

encryption method. A receipt request should be used or requested.

Internet: This data may never be transmitted using a non- MBR Management Corporation 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 MBR Management Corporation 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 Store Support. 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 MBR Management Corporation -approved method. This includes data storage on workstations, systems, backup tapes, etc.

Handling Requirements for Assets and Data Sets Labeled as Essential:

Access: Business need-to-know only. Reviewed quarterly.

Non-Disclosure (NDA): MBR Management Corporation third-parties and employees may only access these assets and data after signing a NDA.

Changes: Changes made to these assets and data sets must follows the MBR Management Corporation Change Management Policy.

Email: Only individuals approved by Store Support to transmit this data may do so, and then only if the email and its attachments are approved using a MBR Management Corporation -approved encryption method. A receipt request should be used or requested.

Internet: This data may never be transmitted using a non- MBR Management Corporation 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 MBR Management Corporation 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 Store Support. 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 MBR Management Corporation -approved method. This includes data storage on workstations, systems, backup tapes, etc.

Handling Requirements for Assets and Data Sets Labeled as Normal:

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 MBR Management Corporation'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 MBR Management Corporation
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.

6.11 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 MBR Management Corporation'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.

6.12 Encryption and Encryption Key Management

Cardholder data is to be retained for the least amount of time needed to support MBR Management Corporation business operations. An important step in protecting this data is to restrict access to it as well as make it unreadable, by hashing, truncation, or encryption. When encryption is used, the correct management of the encryption keys is critical. Should an unauthorized user take advantage of weak encryption key management processes they can unlock the encryption methodology in place to display cardholder data in the clear. Therefore, not only is it important to use strong encryption algorithms in the cardholder environment, but also to safeguard the keys supporting the encryption algorithm for cardholder data being transmitted, processed, and/or stored.

Reference: Encryption and Encryption Key Management Policy.

6.13 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 anytime, or within 10 feet of MBR Management Corporation equipment.

Reference: Equipment Protection Policy.

6.14 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.

6.15 Firewall Configuration and Management

Firewalls are critical to safeguard MBR Management Corporation'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 MBR Management Corporation) and between internal network zones (should one zone contain sensitive systems and the other does not).

Reference: Firewall Configuration and Management Policy.

6.16 Incident Response

Security controls work together to reduce risk in MBR Management Corporation'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 Store Support whenever a suspected incident takes place or there is a system anomaly detected in MBR Management Corporation's cardholder environment.

This allows Store Support to respond to and perform necessary activities to limit damage being caused. MBR Management Corporation 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.

6.17 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 performs 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 Store Support needs to respond immediately to the suspected event and perform forensic, remediation, and then investigative follow-up initiatives. Should an IPS be deployed, Store Support needs to ensure that the attack has been blocked and perform investigative follow-up.

Reference: Intrusion Detection/Prevention Policy.

6.18 Log Management

Logging enables MBR Management Corporation 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, users desktops, applications (as applicable), networking equipment, wireless access points, etc.

Reference: Log Management Policy.

6.19 Password Management

Passwords are the most common method of authenticating the identity of the user before allowing access to systems and applications in MBR Management Corporation'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 MBR Management Corporation policies, and protecting the secrecy of their password. MBR Management Corporation Store Support 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 MBR Management Corporation Store Support is responsible for deploying additional authentication methods as defined by MBR Management Corporation Store Support

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 Store Support 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. Store Support must store user passwords in a secure manner, protected from unauthorized access and in unreadable format.
PULSE PASSWORDS
Please follow the following requirements when setting up your new password:
1. Passwords will be 5 digits
2. Passwords will contain both alpha and numeric characters
3. Passwords will be required to change every 28 days, you will start receiving reminder notices 5 days prior.
4. Passwords can only be repeated every 4 times
5. NEVER enter your password on the touch screen, ALWAYS use the keyboard.
6. Never share or allow someone else to use your password, this is your signature.
7. If you feel that your password has been compromised, change it immediately.
8. Never use another Team Member's password even with their permission
It is your responsibility and duty to use all reasonable care and diligence to maintain the security and confidentiality of your password. Failure to do so may result in disciplinary action up to and including termination of employment and criminal and civil prosecution if applicable. YOU WILL BE HELD RESPONSIBLE FOR ANYTHING THAT OCCURS UNDER YOUR PASSWORD.

Reference: Password Management Policy.

6.20 Physical Security

An unauthorized person may cause physical damage to MBR Management Corporation'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 MBR Management Corporation's facilities or locations which transmit, process, and/or store cardholder data must follow these physical protection policies.

If anyone needs access to the network cabinet, you must notify Store Support using the online form located on **www.mbrdominos.com/IT** DO NOT Share any sensitive data on this form.
Please report anyone that arrives to perform work. Please provide their name, company, date, and time of visit and what they are providing service on. This should include anyone doing maintenance on equipment, utility companies, property management, etc. Report all unexpected visitors, suspicious items or someone tampering with equipment immediately.

Anyone that is requesting access behind the counter and is not expected must be verified **BEFORE** being allowed behind the counter. You should get the person's information and contact your supervisor for further instructions. If your supervisor is not available call Store support at 636-947-4433 x2513. Any suspicious items (USB drives, strange cables, things attached to the cc readers) should be removed and stored in a safe place, stop using the affected equipment, unplug it from the network and power and report immediately. If anyone is seen tampering with computers or network equipment, they must be stopped immediately and reported to store support.

Reference: Physical Security Policy.

6.21 Risk Assessment

The purpose and intent of MBR Management Corporation's security program is to reduce risk as much as possible to MBR Management Corporation's environment, while still enabling MBR Management Corporation 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 MBR Management Corporation Vice President of Finance 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.

6.22 Router Configuration and Management

Routers are an integral part of MBR Management Corporation's network to safeguard MBR Management Corporation'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.

6.23 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 MBR Management Corporation Store Support, 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.

6.24 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 MBR Management Corporation's assets and data, they cannot be held responsible for their actions or know how their actions impact the security of MBR Management Corporation's cardholder environment.

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

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

Reference: Security Awareness Policy.

6.25 Testing and Scanning

Testing MBR Management Corporation's systems and network is a critical component of protecting MBR Management Corporation'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 MBR Management Corporation. 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 MBR Management Corporation'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 MBR Management Corporation to actively try to penetrate systems and applications as if they are an attacker.

Reference: Testing and Scanning Policy.

6.26 Third-Party Access and Management

Threats can be introduced to MBR Management Corporation'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 MBR Management Corporation'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 MBR Management Corporation'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 MBR Management Corporation'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 MBR Management Corporation, but also may be connected to perform non PCI-related functions. Therefore, it is important to safeguard MBR Management Corporation 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 MBR Management Corporation's behalf. MBR Management Corporation maintains primary relationships with DPZ and Worldpay for the purpose/s of POS system and Credit Card processing.

Reference: Third-Party Access and Management Policy.

6.27 Time Synchronization

An accurate clock which synchronizes time across systems is critical to safeguard MBR Management Corporation'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.

7.0 User Signature

Users are to review this Information Security Policy and sign prior to gaining access to MBR Management Corporation's assets and network. Users are then to review and sign this Policy annually as well for the lifetime of their access.

___ New User ___ Annual Signature

User Name: _____

User Title: _____

User Company: _____

User Email: _____

User Phone Number: _____

User Signature: _____

Date: _____

Security Awareness Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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 MBR Management Corporation's assets and data, they cannot be held responsible for their actions or know how their actions impact the security of MBR Management Corporation's cardholder environment. The cardholder environment includes systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

All persons with physical and logical access to MBR Management Corporation's environment, whether employees, third-parties, service providers, contractors, temporary employees, and/or other staff members, must be trained on their role in protecting MBR Management Corporation from threats to help safeguard MBR Management Corporation's finances, operations, and brand name.

Purpose

This Security Awareness Policy details the requirements for the security awareness and training of users with physical and logical access to MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Connection of Users

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

Refresher Training

All users, for the entire length of time they are, or remain, connected to MBR Management Corporation'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.

Logs

Attendance logs for those who attend security awareness training, both, provided upon hire and annually, must be kept by Store Support. 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.

Acknowledgements

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

Security Awareness Vehicles

Supporting vehicles for promoting security awareness are to be maintained throughout the year. These can include newsletter articles, posters, email reminders, and messages acknowledged upon user login.

Technical Training

In addition to the above, those who have admin or privileged access or roles with systems which transmit, process, and store cardholder data must receive additional technical training to further reinforce and supplement their knowledge of security practices.

Testing and Scanning Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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

New vulnerabilities are discovered on a daily basis. Attackers can take advantage of these avenues to launch malicious attacks against MBR Management Corporation. 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 MBR Management Corporation'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 MBR Management Corporation to actively try to penetrate systems and applications as if they are an attacker.

Unauthorized access can potentially lead to a security breach, causing harm to MBR Management Corporation's finances, operations, and brand name.

Purpose

This Testing and Scanning Policy details the requirements for the testing of, and reporting on, vulnerabilities in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by MBR Management Corporation whether located on MBR Management Corporation premises or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Authorization

Prior authorization in writing must be obtained from Store Support before any type of testing is performed of MBR Management Corporation's network and systems. The individual performing the testing must be vetted first to possess the qualifications, experience, and skills to perform such testing. The tools and software used must also be approved by Store Support. No MBR Management Corporation users may ever perform their own testing of any kind on MBR Management Corporation's network, systems, and assets. This is in direct violation with MBR Management Corporation policies.

Scoping

All systems defied as in-scope for the cardholder environment are to be tested and scanned per this policy. All external network connections are to be included in the scope.

Remediation

Findings for any of the types of testing methods below are to be ranked as Critical, High, Medium, or Low, as it relates to the risk assessment results performed for the systems, applications, and data sets in the cardholder environment. This meaning that the risk assessment results correlate with the scan rating results and increase upon sensitivity. Scan findings rated as Critical and High must be remediated within 7, while findings rated as Medium and Low are to be closed within 30 days. Once the findings have been closed, a rescan or retest must be performed to verify that they were closed adequately. MBR Management Corporation Store Support must review these results and provide sign-off.

Retention

All scan and test results, whether initial or remediated findings, must be retained for the purposes of compliance with PCI DSS for a minimum of 5 years. These reports and materials are to be classified as Mission Critical due to the sensitive nature of the content, and handled per the Data Handling and Retention Policies.

Internal Vulnerability Scans

Internal scans are required to be performed on a quarterly basis and may be performed DPZ. Internal scans must be performed on a quarterly basis, at a minimum, and/or after any significant change to the network environment.

External Vulnerability Scans

External scans are required to be performed on a quarterly basis by a PCI authorized third-party scanning vendor (ASV) to meet PCI compliance, however additional external scans performed outside these windows may be performed by a qualified, experienced, and skilled MBR Management Corporation employee. The third-party must review and sign a Non-Disclosure Agreement (NDA) and receive a copy of MBR Management Corporation's information security policies. External scans must be performed on a quarterly basis, at a minimum, and/or after any significant change to the network environment.

Internal and External Penetration Testing

Penetration tests are required to be performed on an annual basis from both the internal and external perspectives. The tests may be performed either by a MBR Management Corporation employee or by a third-party. Both entities are required to provide evidence of their qualifications, skills, experience, and expertise in performing these scans. If a third-party is used, they must review and sign a Non-Disclosure Agreement (NDA) and receive a copy of MBR Management Corporation's information security policies. Internal and external penetration tests must be performed annually, at a minimum, and/or after any significant change to the network environment. The tests must include both the network and the application layers.

Application Testing

Application assessment testing is required to be performed on all internal and external-facing applications in the cardholder environment, unless there is a Web-application firewall placed before the cardholder environment segment. The application testing must be performed by a qualified third-party, and should test against the most recent OWASP Top Ten Web Vulnerabilities List or a similar secure coding framework or guidance. The third-party must review and sign a Non-Disclosure Agreement (NDA) and receive a copy of MBR Management Corporation's information security policies. The application assessment must be performed annually, at a minimum, and/or after any significant change to the network environment.

Wireless Testing

Scanning for the presence of unauthorized wireless access points is to be performed on a quarterly basis, at a minimum, or may be real-time using an intrusion detection/prevention wireless system or similar method. This scanning must occur regardless of whether MBR Management Corporation has wireless in-scope in the cardholder environment or not, and must be performed at all MBR Management Corporation locations. The tests may be performed either by a MBR Management Corporation employee or by a third-party. Both entities are required to provide evidence of their qualifications, skills, experience, and expertise in performing these scans. If a wireless intrusion detection/prevention system is used, it must be configured for real-time alerting and to have these alerts sent to Store Support.

Testing of Third Parties

All third-parties connecting to MBR Management Corporation's network must show evidence that they have performed the scans and tests listed above and have closed any Critical and High vulnerabilities. This evidence is to be provided prior to permitting the third-party access to MBR Management Corporation's network and systems.

.

Third-Party Access and Management Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

Threats can be introduced to MBR Management Corporation'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 MBR Management Corporation'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. MBR Management Corporation'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.

Should an unauthorized user obtain access to MBR Management Corporation's network via this route, they may do so under the pretence 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 MBR Management Corporation'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 MBR Management Corporation, but also may be connected to perform non PCI-related functions. Therefore, it is important to safeguard MBR Management Corporation 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 MBR Management Corporation's behalf. MBR Management Corporation maintains primary relationships with GLS and ControlScan for the purpose/s of Network management and vulnerability scans.

Purpose

This Third-Party Access and Management Policy details the requirements for the evaluation, connection, compliance, and management of third-parties to MBR Management Corporation's cardholder data environment.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned or leased by MBR Management Corporation whether located on MBR Management Corporation premises or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of security controls and practices at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, and temporary employees.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or non-intentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Assessment of Risk

Third-parties must be given a risk assessment prior to being connected to the MBR Management Corporation cardholder data environment. No third-party may be connected to the MBR Management Corporation environment prior to receiving this assessment. Should a third-party have not received this risk assessment and is currently connected, the risk assessment is to be performed before they may be reconnected. This assessment is to include discovery of threats which may lead to potential vulnerabilities, and be an approved vendor in the PCI compliance network.

Once the review has been performed, the third-party is to close gaps found, and the remaining findings and description of risk are to be reviewed and accepted by the Vice President of Finance.

Compliance with the PCI Data Security Standards (PCI DSS) is required for all Level 1 connected third-parties. These entities must have been assessed by an on-site Qualified Security Assessor (QSA), have a Report on Compliance accepted by either their acquiring bank or VISA, and have quarterly passing external scans. Levels 2 - 4 connected third-parties may perform a self-assessment and may be required to have quarterly passing external scans, depending on instruction from their acquiring banks. Should the connected third-party have evidence of their annual PCI compliance passing assessment, they are not required to have a risk assessment performed. Level 1 connected third-parties may provide MBR Management Corporation with their acceptance letter from their acquiring bank or VISA as well as their Attestation of Compliance (AoC). Levels 2 - 4 may provide their Self Assessment Questionnaire (SAQ) and external scans (if performed).

Network Diagram

A network diagram is to be maintained which accurately depicts all connected third-parties, along with networking equipment, systems, applications, wireless networks, and other applicable components of the cardholder data environment.

List of Third-Parties

MBR Management Corporation is to maintain a current list of connected third-parties with details of whether they have direct access to the cardholder environment. This is to clearly denote which third-parties have privileged access and so special attention may be paid to them during session monitoring. The list of third-parties is to also include their PCI compliance status and date of, whether they have accepted by their acquiring bank or VISA or have performed a SAQ (whichever is applicable to their Level as defined above). The list must contain information about which PCI DSS Requirements, if any, are managed by each third-party.

PCI Compliance Status

The status of connected third-parties achieving PCI compliance is to be reviewed annually. All third-parties with direct access to the cardholder environment must obtain PCI compliance or have an official exception provided by their acquiring bank or VISA. Should a third-party with privileged access not have obtained this

compliance status, they are to document in writing their efforts in doing so with the target completion date. MBR Management Corporation is to monitor the compliance efforts of these third-parties.

Terms and Conditions

All connected third-parties are to sign a Non-Disclosure Agreement (NDA). Contracts with Service Providers are to contain terms and conditions, as well as an agreement to safeguard MBR Management Corporation's cardholder data in all its formats from generation to its destruction, and signed by the third-party prior to connection to MBR Management Corporation's network. No third-party may be connected to the MBR Management Corporation environment prior to signing their agreement with MBR Management Corporation's terms and conditions. Should a third-party have not signed their agreement and is currently connected, they are required to do so before they may be reconnected.

Terms and conditions should contain the following, but not limited to, the third-party's obligation to:

- Protect MBR Management Corporation's cardholder data and environment.
- Follow MBR Management Corporation's policies and procedures at all times, unless there is specific approval from Vice President of Finance.
- Use only MBR Management Corporation -approved security controls and practices.
- Communicate any suspected compromise of third-party systems connected to MBR Management Corporation's network.
- Escalate suspected breaches and incidents to the MBR Management Corporation within 24 hours.
- Retain and dispose of electronic and paper cardholder data media in a secure manner.
- Comply with federal and industry laws and regulations.
- Train individuals with access to MBR Management Corporation systems and data on effective safeguard measures.
- Maintain security awareness amongst personnel.
- Conduct criminal background checks on all individuals with access to MBR Management Corporation's network, systems, and data. Background checks are to be performed prior to granting individuals access.
- Removing access permissions immediately upon termination of the individual.
- Maintaining appropriate access control methods, including two-factor remote access.
- Only attempting to connect to MBR Management Corporation's network during authorized periods, and disconnecting when the work is completed.
- Permitting MBR Management Corporation to perform periodic reviews, and forensic investigations upon MBR Management Corporation Vice President of Finance determination.
- Physically and logically segregating MBR Management Corporation systems, networks, and data from those belonging to any other clients.
- Implementing logging and audit trail requirements.
- Notifying and obtaining agreement from MBR Management Corporation prior to outsourcing work to other third-parties.

Change Management

Any changes made by the third-party in regards to their security controls and practices as well as organizational process changes must be communicated to MBR Management Corporation. MBR Management Corporation is to review the change as to its potential impact on MBR Management

Corporation. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from the third-party performing the change is to be reviewed and accepted by the Vice President of Finance.

The email to feedback@mbrmgt.com must be used to track changes from their initial request stage though review to documentation of residual risk to approval by Vice President of Finance.

Any system or application changes with impact on MBR Management Corporation are to be tested by the third-party in a test environment prior to being placed into the production environment.

Event Management and Response

Logs for MBR Management Corporation systems, applications, and equipment managed by the third-parties are to be generated, reviewed, and maintained in accordance with the <Log Management Policy> to provide an audit trail. Logs are to be synced to a safeguarded central location.

Incidents, whether suspected or actual, are to be reported to MBR Management Corporation within 24 hours so they may be responded to in accordance with the <Incident Response Plan>. Determination of the third-party's role in incident response and containment should be clearly defined.

Security Awareness

Training is to be provided by the third-party at an appropriate level by function. Individuals with access to MBR Management Corporation's cardholder environment are to be provided with more detailed training upon hire and then on an annual basis, with a focus on the protection of MBR Management Corporation's cardholder environment and technical training. Other company individuals are to receive general security awareness training upon hire and then annually.

Background Checks

Criminal background checks (within the constraints of local laws) are to be performed by the third-party of each individual with access to MBR Management Corporation's cardholder environment. Background checks should be nation-wide in scope, or at the very least, of each state the individual has resided in.

Access Controls

Access to the MBR Management Corporation's cardholder environment is to be limited to only those individuals with a business need-to-know. Individual authentication, meaning a unique user ID and unique password, is to be used.

Remote access may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their user ID).

Password management is to follow the password requirements specified in the <Password Management Policy>.

Monitoring and Managing Third-Party Access

Third-party access may only be permitted with prior authorization from Director of Store Support and DPZ, and is to be connected immediately after use. Director of Store Support and DPZ are to monitor the access at all times. In some cases, access is granted to third-parties on a 24/7/365 basis. These types of access should be approved by the Vice President of Finance prior to access being granted, and Director of Store Support is to periodically monitor the connection without prior notification to the third-party.

The third-party may not attempt to access MBR Management Corporation's network without prior authorization at anytime, and doing so may result in the initiation of the incident response plan.

Testing and Scanning

The third-party is to agree to periodic security controls and practices review by MBR Management Corporation, and to be included in the vulnerability scanning initiatives performed by MBR Management Corporation and Control Scan. Additional testing procedures, such as penetration testing and application assessments, may also be performed as needed.

In the instance of a breach to MBR Management Corporation's cardholder environment, MBR Management Corporation reserves the right to perform forensic activities on the third-party's environment.

Segregation

The third-party is to logically and physically separate MBR Management Corporation's systems, network, and data from any other clients (if applicable). There may not be any shared environments without the explicit permission of MBR Management Corporation.

Equipment Protection Policy

Version	Date	Change/s	Author/s	Approver/s
2.4	01/07/2024	Store Support	Jason Walls	Jeff Tope

Introduction

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. The physical protection of equipment can help protect MBR Management Corporation data from harsh environment(s) and help safeguard MBR Management Corporation's finances, operations, and brand name.

Purpose

This Equipment Protection Policy details the requirements for the physical protection of equipment in MBR Management Corporation's cardholder data environment for Payment Card Industry (PCI) compliance.

Scope

This policy applies to MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at MBR Management Corporation, whether conducting activities on MBR Management Corporation premises or off-site.

This policy applies to all systems, applications, and equipment owned and/or leased by MBR Management Corporation whether located on MBR Management Corporation premise or off-site, and all MBR Management Corporation locations where cardholder data is present.

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of networking equipment at MBR Management Corporation, to include MBR Management Corporation employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible at 201 N. Main St. Suite 300 Saint Charles, MO 63301 and www.mbrdominos.com

Exceptions

There are no exceptions to this policy. Requests for exceptions may be submitted to the MBR Management Corporation Director of Store Support for review and approval using an email to feedback@mbrmgt.com.

Violations

Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action and possible termination of employment.

Review Schedule

The next scheduled review date is 01/05/2025 by Store Support, to be approved by the Vice President of Finance.

Policy

Assessment of Risk

Equipment should be included in MBR Management Corporation's annual risk assessment process to define its level of sensitivity and security controls required for protection. The assessment should include both, its level of criticality to MBR Management Corporation operations as well as its physical threat potential.

Sitting

Care should be made when situating equipment in locations to protect against potential theft and environmental hazards. These can include loss of power, fire, wind, heat, water and dust. The level of protection should commiserate with the criticality rating of the asset.

Device Inspection

Periodic inspections of these are to take place at regular intervals, with no more than three months passing between inspections. Personnel receive training on how to properly perform device inspections and to recognize signs of tampering. If signs of tampering or damage are found, appropriate steps are taken according to the incident response plan.

Device List

A full list of all devices in use must be maintained. The list is to be promptly updated at the time any changes occur.

Make and Model	Device Location	Serial Number

Data Centers or Computer Rooms

Access to data centers or computer rooms must follow the requirements in the MBR Management Corporation Physical Access Security Policy. Additional protective measures should be in place on equipment which is deemed critical, such as console locks.

Food and Beverages

Food and beverages may not be brought into data centers or computer rooms at anytime, or within 10 feet of MBR Management Corporation equipment.

Environmental Controls

The following should be in place to protect MBR Management Corporation equipment, at a minimum:

Loss of power:	Uninterruptable Power Supply (UPS)
Extreme temperature:	Temperature and humidity monitoring
Heat and smoke detection:	Fire detection systems
Heat and smoke suppression:	Fire extinguisher systems (or other suppression methods)

Cables

Any/all Cabling is to be routed either under the floor or above the equipment so they are inaccessible and safe from unintentional hazard.

Maintenance Inspections

Vendor guidelines are to be followed while setting up equipment and while performing inspections. Equipment should be inspected, at a minimum, on an annual basis and must be performed by authorized individuals only. Deployment, maintenance, and inspection records and logs are to be retained for the life of the equipment.