MINDBODY Merchant PCI DSS Requirements

MINDBODY, Booker, FitMetrix, and BowTie.ai

2019-2020

Introduction

To provide merchants leveraging MINDBODY Inc. (MINDBODY) additional clarity on regulatory requirements, and as required by the requirement 12.8.2, the following outlines responsibilities of MINDBODY and customers who utilize specific MINDBODY Merchant payment flows with regards to the Payment Card Industry Data Security Standard (PCI DSS).

As a trusted partner processing cardholder data on behalf of merchants, MINDBODY, inclusive of its affiliated platforms of Booker, FitMetrix, Bowtie and Frederick, is certified as a Level 1 Service Provider under PCI DSS Version 3.2. MINDBODY last underwent their annual certification by the third-party Qualified Security Assessor Company (QSAC) PSC on September 30, 2019 and was found to be compliant with an annual Attestation of Compliance (AOC) issued as valid until September 29, 2020. A copy of MINDBODY's AOC is available upon request.

The use of MINDBODY's technology and services can greatly assist with reducing the burden of regulatory compliance but does not fully absolve merchants from requirements within the PCI DSS. While each use case of MINDBODY is unique, the following document captures typical use cases of MINDBODY's platform and the applicable requirements. [NOTE: This document is not legal advice. We urge you to consult your own legal counsel to familiarize yourself with the requirements that govern your own specific situation.]

Definitions

The following terms are utilized throughout the document as defined:

Cardholder Data – The account number, card verification code, magnetic track data, or chip data found on credit and debit cards backed by Visa, MasterCard, Discover, American Express, or JCB networks.

Merchant – The studio, provider, or other entity which provides goods or services and accepts cardholder data through services and technology provided by MINDBODY.

Consumers – The customers of merchants receiving goods or services who leverages a credit or debit card for payment.

What is PCI DSS and What Is Required?

The Payment Card Industry Data Security Standard (PCI DSS) outlines a set of security and industry requirements for the handling of cardholder data backed by the major card brand networks (Visa, MasterCard, Discover, American Express, and JCB). Any merchant or service provider who stores, processes, transmits or otherwise impacts the security of cardholder data is required to comply with the technical and procedural controls outlined in the standard on an ongoing basis and certify their compliance on an annual basis.

The methods and level of requirement are set forth by the merchant bank that settles the processing of your transactions and is not determined by MINDBODY. For the majority of MINDBODY Merchants, annual attestation of compliance by way of a Self-Assessment Questionnaire (SAQ) is required between the merchant and their merchant bank. In a more limited number of situations, a full Report on Compliance may be required by your Merchant Bank and requires the certification by a PCI QSAC.

More information on the types of Self-Assessment Questionnaires and requirements can be found on the PCI SSC's website: https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

Overview of MINDBODY's Responsibilities

MINDBODY provides business management SaaS offerings to the health and wellness community with payments occurring through MINDBODY's platform and payment partner platforms. MINDBODY services allow a Merchant the ability to process and store cardholder data for the purpose of point of sale transactions, e-commerce, and reoccurring subscription transactions.

Given the service offerings and methods in which MINDBODY stores, processes, and transmits cardholder data, MINDBODY maintains the responsibility for all applicable PCI DSS requirements for cardholder data provided directly from Consumers to MINDBODY.

For cardholder data provided to MINDBODY by Merchants on behalf of Consumers, MINDBODY is responsible for all requirements upon the receipt of cardholder data. MINDBODY is not responsible for the security of cardholder data being processed by Merchants until it is received by MINDBODY's systems. For the abundance of clarity, this means merchants are responsible for all applicable PCI DSS requirements on the systems, networks, and facilities they use to connect to MINDBODY's services to provide cardholder data.

For Merchants leveraging additional methods of accepting cardholder data outside of MINDBODY provided services (such as other point of sale, e-commerce, or billing solutions), additional consideration is required for the responsibility of each leveraged service.

MINDBODY

Common Use Cases and Compliance Requirements*

As previously mentioned, MINDBODY is responsible for all applicable PCI DSS requirements upon the receipt of cardholder data by MINDBODY's systems and services. As several methods for the storage, processing, and transmitting cardholder data exist, the following matrix outlines the Self-Assessment Questionnaires commonly requested by merchant banks, the relevant scope of Merchant responsbilities, and considerations for common use cases where the Merchant directly processes cardholder data.

* This matrix is not legal advice and does not guarantee your own compliance with PCI DSS requirements. We urge you to consult your own legal counsel to familiarize yourself with the requirements that govern your own specific situation.

Methods of Processing Cardholder Data	Merchant Responsibilities		Notes and Considerations
	SAQ	Primary Scope	
Direct from Consumers to MINDBODY ***MINDBODY, Booker, FitMetrix, and Bowtie*** Merchants never direct nor process cardholder data and direct Consumers directly to an application or service hosted by MINDBODY.	**SAQ A**	**Policy and Procedures Only** Requirement 12.8	As Consumers provide MINDBODY's services cardholder data directly, all technical requirements applicable to the methods of processing are the responsibility of MINDBODY. Merchants are required to monitor MINDBODY's continued compliance annually.
Merchant Website with Integrated MINDBODY IFrame ***MINDBODY and Booker*** Merchants provide Consumers a seamless experience by integrating a widget within their own website domain to provide cardholder data and complete the transaction. **Merchant's Website with Integrated JavaScript** ***Bowtie*** Merchants have Bowtie integrated into their website for web chat functionality.	**SAQ A-EP**	**Website Hosting** Technical requirements required on web hosting provider and Merchant's configuration of their site	Given the Merchant's website has the ability to direct where Consumers provide their cardholder data, controls are required to protect the integrity of the desired flow and ensure cardholder data is not intercepted. It is recommended to consider leveraging a provider who offers managed hosting in an environment assessed as PCI DSS Compliant (and can provide a PCI DSS Service Provider AOC).
Card-Not-Present Merchant Processing ***MINDBODY and Booker*** Merchants manually enter cardholder data that is either received by phone or in-person with a computer or mobile device into a MINDBODY website.	**SAQ C-VT**	**Computers and Mobile Devices** Technical controls are required to protect the security of the systems submitting cardholder data to MINDBODY	With Merchants entering cardholder data into a system controlled by them, PCI DSS focuses on the security of the system to protect keystroke logging or other malware from capturing keyed-in cardholder data.
Merchant Card-Present using Clover, Magtek, or Unimag2 ***MINDBODY and Booker***	**SAQ B-IP**	**Physical Security of Terminals** Regular inspection of devices	As the provided readers leverage end-to-end encryption, PCI DSS requirements focus on the

Methods of Processing Cardholder Data	Merchant Responsibilities		Notes and Considerations
	SAQ	Primary Scope	
		recommended as well as implementing procedures to protect against tampering or unauthorized replacement.	physical security of the readers to prevent tampering or skimming of track data.
Merchant Card-Present using Legacy USB or Headphone Mobile Phone Readers ***MINDBODY***	**SAQ C**	**Computers and Mobile Devices** **Physical Security of Terminals** Technical controls are required to protect the security of the systems submitting cardholder data to MINDBODY	These readers do not leverage encryption to protect cardholder data, and as such, additional controls may be required in addition to the SAQ C-VT given the nature of the processing.
Multiple Methods Indicating Differing SAQs ***All MINDBODY Brands*** Given the functionality of MINDBODY offerings, cardholder data is accepted using multiple methods outlined above and fall under multiple SAQs. **Methods External To MINDBODY** ***Non-MINDBODY 3rd Party Methods*** In addition to MINDBODY, the Merchant utilizes their account to process cardholder data in 3rd party non-MINDBODY applications with multiple methods.	**SAQ D or Various**	**As Listed Above**	The determination of which SAQ or applicable requirements apply to you is ultimately the decision of your merchant bank. As such, it is recommended to discuss with your merchant bank which of the following is required: **Multiple SAQs** – The merchant bank may accept the completion of multiple SAQs relevant to each individual flow simplifying the complexity of requirements. **SAQ D –**This version of the SAQ contains the greatest number of requirements.

MINDBODY

PCI DSS Requirement 1*

Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

* The following matrices (Requirements 1-12) are not legal advice and do not guarantee your own compliance with PCI DSS requirements. We urge you to consult your own legal counsel to familiarize yourself with the requirements that govern your own specific situation.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations						A documented and implemented process for approving and testing all connections and changes to the firewalls and routers may help prevent security problems caused by misconfiguration of the network, router, or firewall.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks						Network diagrams describe how networks are configured and identify the location of all network devices.
1.1.3 Current diagram that shows all cardholder data flows across systems and networks						Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network.
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone						Using a firewall on every Internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.
1.1.5 Description of groups, roles, and responsibilities for management of network components						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.						Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						business, organizations can help ensure that all other services, protocols, and ports are disabled or removed. If insecure services, protocols, or ports are necessary for business, the risk posed by the use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed.
1.1.7 Requirement to review firewall and router rule sets at least every six months						This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment and specifically deny all other traffic.						Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This can help prevent malicious individuals from accessing the

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within the entity's network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.
1.2.2 Secure and synchronize router configuration files.						While the running (or active) router configuration files include the current, secure settings, the startup files (which are used when routers are re-started or booted) must be updated with the same secure settings to ensure these settings are applied when the start-up configuration is run.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.						The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and cardholder data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the Cardholder Data Environment (CDE), malicious individuals that gain unauthorized

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						access to the wireless network can easily connect to the CDE and compromise account information. Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include but is not limited to, corporate networks, retail stores, guest networks, warehouse environments, etc.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.						
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.						The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), and services that an organization needs to have available to the public (like a web server).
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.						This functionality is intended to help prevent malicious individuals from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)						Normally a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet came from. Malicious individuals will often try to spoof (or imitate) the sending IP address so that the target system

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						believes the packet is from a trusted source. Filtering packets coming into the network helps to, among other things, ensure packets are not "spoofed" to look like they are coming from an organization's own internal network.
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.						All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).
1.3.5 Permit only "established" connections into the network.						A firewall that maintains the "state" (or the status) for each connection through the firewall should know whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection's status) or is malicious traffic trying to trick the firewall into allowing the connection.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.						**Commonly Not Applicable** When leveraging MINDBODY solely for the storage of cardholder data, MINDBODY is responsible for this control. Merchants should not store cardholder data in digital formats outside of leveraging MINDBODY and may need to address this requirement if

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						leveraging additional storage outside of MINDBODY.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.						Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network and using that information to access the network. Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.						Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is reconnected to the network.
1.5 Ensure that security policies and operational procedures for managing firewalls are						Personnel needs to be aware of and follow security policies and operational procedures to help ensure firewalls and

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
documented, in use, and known to all affected parties.						routers are continuously managed to prevent unauthorized access to the network.

PCI DSS Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.						Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings may help reduce a system's vulnerability to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will help prevent a malicious individual from re-enabling the account and gaining access with the default password.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.						If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. In addition, the key-exchange protocol for older versions of 802.11x encryption

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						(Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.						There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, several security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses. Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov, www.sans.org, and www.cisecurity.org, www.iso.org, and product vendors. System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)						If server functions that need different security levels are located on the same server, the security level of the functions with higher security needs would be reduced due to the presence of the lower-security functions. Additionally, the server functions with a lower security level may introduce security weaknesses to other functions on the same server. By considering the security

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						needs of different server functions as part of the system configuration standards and related processes, organizations can ensure that functions requiring different security levels don't co-exist on the same server.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.						As stated in Requirement 1.1.6, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. Including this requirement as part of an organization's configuration standards and related processes helps ensure that only the necessary services and protocols are enabled.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.						Enabling security features before new servers are deployed may help prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.).

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
2.2.4 Configure system security parameters to prevent misuse.						System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.						Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. By removing unnecessary functionality, organizations can focus on securing the functions that are required and reduce the risk that unknown functions will be exploited. Including this in server-hardening standards and processes can help address the specific security implications associated with unnecessary functions (for example, by removing/disabling FTP or the web server if the server will not be performing those functions).
2.3 Encrypt all non-console administrative access using strong cryptography.						If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's IDs and

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring a SAQ-D and is not required for the SAQs listed here.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.						Personnel need to be aware of and follow security policies and daily operational procedures to help ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.

MINDBODY

PCI DSS Requirement 3

Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.						**Commonly Not Applicable** When leveraging MINDBODY solely for the storage of cardholder data, MINDBODY is responsible for this control. Merchants should not store cardholder data in digital formats outside of leveraging MINDBODY and may need to address this requirement if leveraging additional storage outside of MINDBODY.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.						Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:						them to generate counterfeit payment cards and create fraudulent transactions. .
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for the business.*						If full track data is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions.
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.						The purpose of the card validation code is to protect "card-not-present" transactions—Internet or mail order/telephone order (MO/TO)

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						transactions—where the consumer and the card are not present. If this data is stolen, malicious individuals can execute fraudulent Internet and MO/TO transactions.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.						These values should be known only to the card owner or bank that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based debit transactions (for example, ATM withdrawals).
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.						MINDBODY's services and systems adhere to this requirement.
Requirements 3.4 – 3.7 Various Controls						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.

MINDBODY

PCI DSS Requirement 4

Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates, are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.						Sensitive information must be encrypted during transmission over public networks because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted. Note that some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent the use of an insecure connection—for example, by using only trusted certificates and supporting only

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						strong encryption (not supporting weaker, insecure protocols or methods). Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection. Generally, the web page URL should begin with "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser. Many TLS certificate vendors also provide a highly visible verification seal— sometimes referred to as a "security seal," "secure site seal," or "secure trust seal")—which may provide the ability to click on the seal to reveal information about the website.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.						Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks. Strong cryptography for authentication and transmission of cardholder data is required to help prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).						E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Do not

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						utilize these messaging tools to send PAN unless they are configured to provide strong encryption. Additionally, if an entity requests PAN via end-user messaging technologies, the entity should provide a tool or method to protect these PANs using strong cryptography or render PANs unreadable before transmission.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.						Personnel needs to be aware of and follow security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

PCI DSS Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

Malicious software commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).						There is a constant stream of attacks using widely published exploits, often called "zero-day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. Without an anti-virus solution that is updated regularly, these new forms of malicious software can attack systems, disable a network, or lead to the compromise of data.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.						It is important to protect against ALL types and forms of malicious software.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.						Industry trends for malicious software can change quickly, so organizations need to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-virus news groups to determine whether their systems might be coming under threat from new and evolving malware. Trends in malicious software should be included in the identification of new

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed.
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.						Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.						Anti-virus software that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active—for example, disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after it is re-enabled.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.						Personnel needs to be aware of and follow security policies and operational procedures to ensure systems are protected from malware continuously.

MINDBODY

PCI DSS Requirement 6

Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to help protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.						The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment. Sources for vulnerability information should be trustworthy and often include vendor websites, industry newsgroups, mailing list, or RSS feeds. Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must, therefore, have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities. This is not achieved by an ASV scan or internal vulnerability scan; rather this requires a process to actively monitor industry sources for vulnerability information. Classifying the risks (for example, as "high," "medium," or "low") allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						vulnerabilities posing the greatest risk will be exploited.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.						There is a constant stream of attacks using widely published exploits, often called "zero-day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system or gain access to sensitive data. Prioritizing patches for critical infrastructure will help ensure that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. This requirement applies to applicable patches for all installed software, including payment applications (both those that are Payment Application Data Security Standard (PA-DSS) validated and those that are not).
Requirements 6.3 – 6.4.4 Various Requirements						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
6.4.5 Change control procedures must include the following:						If not properly managed, the impact of system changes—such as hardware or software updates and installation of security patches—might not be fully realized and could have unintended consequences.
6.4.5.1 Documentation of impact.						The impact of the change should be documented so that all affected parties can plan appropriately for any processing changes.
6.4.5.2 Documented change approval by authorized parties.						Approval by authorized parties indicates that the change is a legitimate and approved change sanctioned by the organization.
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.						Thorough testing should be performed to verify that the security of the environment is not reduced by implementing a change. Testing should validate that all existing security controls remain in place, are replaced with equally strong controls, or are strengthened after any change to the environment.
6.4.5.4 Back-out procedures.						For each change, there should be documented back-out procedures in case the change fails or adversely affects the security of an application or system, to allow the system to be restored to its previous state.
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and						Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
networks, and documentation updated as applicable.						applied to any systems or networks added or changed within the in-scope environment. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date, and security controls are applied where needed. A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process.
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines.						The application layer is high-risk and may be targeted by both internal and external threats. Requirements 6.5.1 through 6.5.10 are the minimum controls that should be in place, and organizations should incorporate the relevant secure coding practices as applicable to the particular technology in their environment. Application developers should be properly trained to identify and resolve issues related to these (and other) common coding vulnerabilities. Having staff knowledgeable of secure coding guidelines could minimize the number of security vulnerabilities introduced through poor coding practices. Training for developers may be provided in-house or by third parties and should be relevant to the technology used.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						As industry-accepted secure coding practices change, organizational coding practices and developer training should likewise be updated to address new threats—for example, memory scraping attacks.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.						Injection flaws, particularly SQL injection, are a commonly used method for compromising applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data and allows the attacker to attack components inside the network through the application, to initiate attacks such as buffer overflows, or to reveal both confidential information and server application functionality. Information should be validated before being sent to the application—for example, by checking for all alpha characters, a mix of alpha and numeric characters, etc.
6.5.2 Buffer overflows						Buffer overflows occur when an application does not have appropriate bounds checking on its buffer space. This can cause the information in the buffer to be pushed out of the buffer's memory space and into executable memory space. When this occurs, the attacker can insert malicious code at the end of the buffer and then push that malicious code into executable memory

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						space by overflowing the buffer. The malicious code is then executed and often enables the attacker remote access to the application and/or infected system.
6.5.3 Insecure cryptographic storage						**Commonly Not Applicable** When leveraging MINDBODY solely for the storage of cardholder data, MINDBODY is responsible for these applicable controls. Merchants should not store cardholder data in digital formats outside of leveraging MINDBODY and may need to address this requirement if leveraging additional storage outside of MINDBODY.
6.5.4 Insecure communications						Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain control of an application or even gain clear-text access to encrypted data.
6.5.5 Improper error handling						Applications can unintentionally leak information about their configuration or internal workings or expose privileged information through improper error handling methods. Attackers use this weakness to steal sensitive data or compromise the system altogether. If a malicious individual can create errors that the application does not handle properly, they can gain detailed system

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						information, create denial-of-service interruptions, cause security to fail, or crash the server. For example, the message "incorrect password provided" tells an attacker the user ID provided was accurate and that they should focus their efforts only on the password. Use more generic error messages, like "data could not be verified."
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).						All vulnerabilities identified by an organization's vulnerability risk-ranking process (defined in Requirement 6.1) to be "high risk" and that could affect the application should be identified and addressed during application development.
6.5.7 Cross-site scripting (XSS)						XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser, which can hijack user sessions, deface web sites, possibly introduce worms, etc.
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).						A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization. Consistently enforce access control in the presentation layer and business

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						logic for all URLs. Frequently, the only way an application protects sensitive functionality is by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly. An attacker may be able to enumerate and navigate the directory structure of a website (directory traversal) thus gaining access to unauthorized information as well as gaining further insight into the workings of the site for later exploitation.
6.5.9 Cross-site request forgery (CSRF)						A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then enables the attacker to perform any state-changing operations the victim is authorized to perform (such as updating account details, making purchases, or even authenticating to the application).
6.5.10 Broken authentication and session management						Secure authentication and session management helps prevent unauthorized individuals from compromising legitimate account credentials, keys, or session tokens that would otherwise enable the intruder to assume the identity of an authorized user.
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing						Public-facing web applications are primary targets for attackers, and poorly

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.						coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to help reduce the number of compromises on public-facing web applications due to poor coding or application management practices.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.						Personnel needs to be aware of and follow security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities continuously.

PCI DSS Requirement 7

Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.						
7.1.1 Define access needs for each role, including • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.						**Commonly Not Applicable** When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for this control. Merchants may need to address this requirement if leveraging additional storage outside of MINDBODY.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.						When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall system administrator. Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						if an unauthorized person gains access to a user ID.
7.1.3 Assign access based on individual personnel's job classification and function.						Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easier to grant individuals access according to their job classification and function by using the already-created roles.
7.1.4 Require documented approval by authorized parties specifying required privileges.						Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management and that their access is necessary for their job function.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:						
7.2.1 Coverage of all system components						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
7.2.2 Assignment of privileges to individuals based on job classification and function.						
7.2.3 Default "deny-all" setting.						
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.						

MINDBODY

PCI DSS Requirement 8

Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Requirements 8.1.1, 8.1.6 through 8.1.8, 8.2, 8.5, and 8.2.3 through 8.2.5are not intended to apply to user accounts within a point-of-sale payment application that only has access to one card number at a time to facilitate a single transaction (such as cashier accounts).

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:						
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.						By ensuring each user is uniquely identified— instead of using one ID for several employees—an organization can help maintain individual responsibility for actions and an effective audit trail per employee. This will help facilitate issue resolution and containment when a misuse or malicious intent occurs.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.						To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
8.1.3 Immediately revoke access for any terminated users.						If an employee has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account. To prevent unauthorized access, user credentials, and other authentication methods, therefore, need to be revoked promptly (as soon as possible) upon the employee's departure.
8.1.4 Remove/disable inactive user accounts within 90 days.						Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the period needed and disabled when not in use. • Monitored when in use.						Allowing vendors to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed and disabling it as soon as it is no longer needed, helps prevent misuse of these connections. Monitoring of vendor access provides assurance that vendors are accessing

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						only the systems necessary and only during approved time frames.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.						Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.						If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the admin or help desk can validate that it is the actual account owner requesting reactivation.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.						When users walk away from an open machine with access to critical system components or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. The re-authentication can be applied either at the system level to protect all sessions running on that machine, or at the application level.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.						These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.						Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored and use this data to gain unauthorized access.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.						Many malicious individuals use "social engineering"—for example, calling a help desk and acting as a legitimate user—to have a password changed so they can utilize a user ID. Consider the use of a "secret question" that only the proper user can answer to help administrators identify the user prior to re-setting or modifying authentication credentials.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.						Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. For cases where this minimum cannot be met due to technical limitations, entities may use "equivalent strength" to evaluate their alternatives. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards.
8.2.4 Change user passwords/passphrases at least once every 90 days.						Passwords/passphrases that are valid for a long time without a change provide malicious individuals with more time to work on breaking the password/phrase.
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.						If password history isn't maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period of time reduces the likelihood that passwords that have been guessed or brute-forced will be used in the future.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.						If the same password is used for every new user, an internal user, former employee, or malicious individual may know or easily discover this password and use it to gain access to accounts.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*					
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.						This requirement is intended to apply to all personnel with non-console administrative access to the CDE. If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use multi-factor authentication either when logging onto the CDE network or when logging onto a system. If the CDE is segmented from the rest of the entity's network, an administrator would need to use multi-factor authentication when connecting to a CDE system from a non-CDE network. Multi-factor authentication can be implemented at the network level or at the system/application level.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator and including third party access for support or maintenance) originating from outside the entity's network.						This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance)—with remote access to the network where that remote access could lead to access to the CDE. MFA is required for any

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						remote access to networks with access to the cardholder data environment and is recommended for all remote access to the entity's networks.
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.						Communicating password/authentication policies and procedures to all users help those users understand and abide by the policies. For example, guidance on selecting strong passwords may include suggestions to help personnel select hard-to-guess passwords that don't contain dictionary words, and that doesn't contain information about the user (such as the user ID, names of family members, date of birth, etc.). Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files, and being alert for malicious individuals who may attempt to exploit their passwords (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem"). Instructing users to change passwords if there is a chance the password is no longer secure can help prevent malicious users from using a legitimate password to gain unauthorized access.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed.						If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This, in turn,

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
• Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.						prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.						If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account can help prevent unauthorized users from gaining access through the use of a shared authentication mechanism.
8.7 All-access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).						**Commonly Not Applicable** When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for this control. Merchants may need to address this requirement if leveraging additional storage outside of MINDBODY.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.						Personnel needs to be aware of and follow security policies and operational procedures for managing identification and authorization continuously.

MINDBODY

PCI DSS Requirement 9

Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.						Without physical access controls, such as badge systems and door controls, unauthorized persons could potentially gain access to the facility to steal, disable, disrupt, or destroy critical systems and cardholder data. Locking console login screens helps prevent unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.						When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited. Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned, so they are out of reach and/or be monitored to detect tampering. Similarly, access control

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						mechanisms could be monitored or have physical protections installed to prevent them from being damaged or disabled by malicious individuals.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.						Restricting access to network jacks (or network ports) may help prevent malicious individuals from plugging into readily available network jacks and gain access into internal network resources. Whether logical or physical controls or a combination of both, are used, they should be sufficient to prevent an individual or device that is not explicitly authorized from being able to connect to the network.
Requirements 9.1.3 – 9.4.4 Various Requirements						When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for these applicable controls. Merchants may need to address these requirements if leveraging additional storage outside of MINDBODY.
9.5 Physically secure all media.						Controls for physically securing media are intended to help prevent unauthorized persons from gaining access to cardholder data on different types of media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.						When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for these applicable controls. Merchants may need to address these requirements if leveraging additional storage outside of MINDBODY.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:						Procedures and processes help protect cardholder data on media distributed to internal and/or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes.
9.6.1 Classify media so the sensitivity of the data can be determined.						Media must be identified such that its classification status can be easily discernible. Media not identified as confidential may not be adequately protected or may be lost or stolen.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.						Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).						Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media may not be tracked or appropriately protected, and its location would be unknown,

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						potentially leading to lost or stolen media.
9.7 Maintain strict control over the storage and accessibility of media.						Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.						When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for these applicable controls. Merchants may need to address these requirements if leveraging additional storage outside of MINDBODY.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:						If steps are not taken to destroy information contained on hard disks, portable drives, CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed of media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack.
9.8.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.						Securing storage containers used for materials that are going to be destroyed helps prevent sensitive information from being captured while the materials are being collected. For example, "to-be-shredded" containers could have a lock preventing access to

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						its contents or physically prevent access to the inside of the container.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.						When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for these applicable controls. Merchants may need to address these requirements if leveraging additional storage outside of MINDBODY.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	***Note**: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*					
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or another method of unique identification.						Keeping an up-to-date list of devices helps an organization keep track of where devices are supposed to be, and quickly identify if a device is missing or lost. The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned.
9.9.2 Periodically inspect device surfaces to detect tampering (for example, the addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).						Regular inspections of devices will help organizations to more quickly detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices. The type of inspection will depend on the device— for example, photographs

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						of devices that are known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace the outer casing of a device to hide their tampering, and these methods may help to detect such activities. Device vendors may also be able to provide security guidance and "how to" guides to help determine whether the device has been tampered with.
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).						Criminals will often pose as authorized maintenance personnel in order to gain access to POS devices. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POS maintenance company (such as the vendor or acquirer) for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in workwear), and could also be knowledgeable about locations of devices, so it's important that personnel are trained to follow procedures at all times. Another trick criminals like to use is to send a "new" POS system with

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						instructions for swapping it with a legitimate system and "returning" the legitimate system to a specified address. The criminals may even provide return postage as they are very keen to get their hands on these devices. Personnel should always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business.
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.

PCI DSS Requirement 10

Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
10.1 Implement audit trails to link all access to system components to each individual user.						It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.
10.2 Implement automated audit trails for all system components to reconstruct the following events:						
10.2.1 All individual user accesses to cardholder data						When leveraging MINDBODY solely for the processing of cardholder data, MINDBODY is responsible for these applicable controls. Merchants may need to address these requirements if leveraging additional storage outside of MINDBODY.
10.2.2 All actions were taken by any individual with root or administrative privileges						Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						privilege back to the specific action and individual.
10.2.3 Access to all audit trails						Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having access to logs identifying changes, additions, and deletions can help retrace steps made by unauthorized personnel.
10.2.4 Invalid logical access attempts						Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges						Without knowing who was logged on at the time of an incident, it is very difficult to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
10.2.6 Initialization, stopping, or pausing of the audit logs						Turning the audit logs off (or pausing them) before performing illicit activities is a common practice for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
10.2.7 Creation and deletion of system-level objects						Malicious software, such as malware, often creates or replaces system-level objects on the target system to control a particular function or operation on that system. By logging when system-level objects, such as database tables or stored procedures, are created or deleted, it will be easier to determine whether such modifications were authorized.
10.3 Record at least the following audit trail entries for all system components for each event:						
10.3.1 User identification						By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with hopefully sufficient detail to know who, what, where, when, and how.
10.3.2 Type of event						
10.3.3 Date and time						
10.3.4 Success or failure indication						
10.3.5 Origination of event						
10.3.6 Identity or name of affected data, system component, or resource.						
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.						Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic
10.4.1 Critical systems have the correct and consistent time.						

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
10.4.2 Time data is protected.						analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.
10.4.3 Time settings are received from industry-accepted time sources.						
10.5 Secure audit trails so they cannot be altered.						
10.5.1 Limit viewing of audit trails to those with a job-related need.						Adequate protection of the audit logs include strong access control (limit access to logs based on "need to know" only) and use of physical or network segregation to make the logs harder to find and modify. Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.
10.5.2 Protect audit trail files from unauthorized modifications.						
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.						
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.						By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Logs may be written directly, or offloaded or copied from external systems, to the secure internal system or media.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating						File-integrity monitoring or change-detection systems check for changes to critical files and notify when such changes are noted. For file-integrity

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
alerts (although new data being added should not cause an alert).						monitoring purposes, an entity usually monitors files that don't regularly change, but when changed, indicate a possible compromise.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.						
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).						Checking logs daily minimizes the amount of time and exposure of a potential breach. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that determination of a "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior.
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.						Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						determined by an entity's annual risk assessment.
10.6.3 Follow up exceptions and anomalies identified during the review process.						If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).						Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having at least three months of logs immediately available, an entity can more quickly identify and minimize the impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.
Requirements 10.8 – 10.8.1 Not Applicable – Service Providers Only						
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.

MINDBODY

PCI DSS Requirement 11

Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
11.1 Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.						Implementation and/or exploitation of wireless technology within a network are some of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, it can allow an attacker to easily and "invisibly" enter the network. Unauthorized wireless devices may be hidden within or attached to a computer or other system component or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment. Knowing which wireless devices are authorized can help administrators more quickly identify unauthorized wireless devices and responding to the identification of unauthorized wireless access points can help to proactively minimize the exposure of the CDE to malicious individuals.
11.1.1 Maintain an inventory of authorized wireless access points, including a documented business justification.						
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.						
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new						

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
system component installations, changes in network topology, firewall rule modifications, product upgrades).						
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.						An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked "High" per Requirement 6.1) should be resolved with the highest priority.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.						As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV). A robust scanning program can help ensure that scans are performed, and vulnerabilities addressed promptly.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.						The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Scanning an environment after any significant changes are made can help ensure that changes were completed appropriately such that the security of the environment was not compromised as a result of the change. All system

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						components affected by the change will need to be scanned.
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.						The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This can allow an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks.
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).						Penetration testing conducted on a regular basis and after significant changes to the environment is a proactive security measure that can help minimize potential access to the CDE by malicious individuals.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected, and testing is repeated to verify the corrections.						The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Performing penetration tests after network upgrades and modifications can help provide assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.						Penetration testing is an important tool to confirm that any segmentation in place to isolate the CDE from other networks is effective. The penetration testing should focus on the segmentation controls, both from outside the entity's network and from inside the network but outside of the CDE, to confirm that they are not able to get through the segmentation controls to access the CDE. For example, network testing and/or scanning for open ports, to verify no connectivity

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						between in-scope and out-of-scope networks.
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.						Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real-time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.						Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and can notify you when such changes are detected. If not implemented properly or the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.						
11.6 Ensure that security policies and operational procedures for security monitoring and testing are						**Not Applicable for Most SAQs**

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
documented, in use, and known to all affected parties.						As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.

MINDBODY

PCI DSS Requirement 12

Maintain a policy that addresses information security for all personnel

A strong security policy helps set the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
12.1 Establish, publish, maintain, and disseminate a security policy.						A company's information security policy influences the roadmap for implementing security measures to help protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.						Security threats and protection methods evolve rapidly. Without updating the security policy to reflect relevant changes, new protection measures to fight against these threats are not addressed.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk.						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
12.3 Develop usage policies for critical technologies and define proper use of these technologies.						

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
12.3.1 Explicit approval by authorized parties						Without requiring proper approval for implementation of these technologies, individual personnel may innocently implement a solution to a perceived business need, but may also open a huge security hole that subjects critical systems and data to malicious individuals.
12.3.2 Authentication for use of the technology						If technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), malicious individuals may easily use this unprotected technology to access critical systems and cardholder data.
12.3.3 A list of all such devices and personnel with access						Malicious individuals may breach physical security and place their own devices on the network as a "back door." Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quicker identification of non-approved installations.
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)						As of PCI DSS 3.2.1, these requirements are not required for the applicable SAQs. Merchants may be required to address these requirements if completing an SAQ-D.
12.3.5 Acceptable uses of the technology						By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to help ensure a "back door" is not
12.3.6 Acceptable network locations for the technologies						

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						opened for a malicious individual to gain access to critical systems and cardholder data.
12.3.7 List of company-approved products						As of PCI DSS 3.2.1, these requirements are not required for the applicable SAQs. Merchants may be required to address these requirements if completing an SAQ-D.
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity						Remote-access technologies are frequent "back doors" to critical resources and cardholder data. By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS vendor, other vendors, or business partners), access and risk to networks can be minimized.
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use						
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, these requirements are not required for the applicable SAQs. Merchants may be required to address these requirements if completing an SAQ-D.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.						Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to the insecure implementation of

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						technologies or use of outdated or insecure technologies.
12.5 Assign to an individual or team the following information security management responsibilities:						
Requirements 12.5.1 – 12.5.2 Not Applicable						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, these requirements are not required for the applicable SAQs. Merchants may be required to address these requirements if completing an SAQ-D.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.						Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.
12.5.4 – 12.5.5 Not Applicable						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.						If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.
Requirements 12.6.1 – 12.7 Not Applicable						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
12.8 Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows						
12.8.1 Maintain a list of service providers including a description of the service provided.						If a merchant or service provider shares cardholder data with a service provider, certain requirements may apply to ensure continued protection of this data will be enforced by such service providers. Some examples of different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, entities that receive data for fraud-modeling purposes, etc. Keeping track of all service providers can help identify where potential risk extends to outside of the organization.

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
12.8.2 Maintain a written agreement that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.						The acknowledgment of the service providers can evidence their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity. In conjunction with Requirement 12.9, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.
12.8.3 Ensure there is an established process for engaging service providers, including proper due diligence prior to engagement.						The process can help ensure that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider. Specific due-diligence processes and goals will vary for each organization. Examples of considerations may include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
						validates their PCI DSS compliance and what evidence they will provide, etc.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.						Knowing your service providers' PCI DSS compliance status can help provide assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and those services in scope for the client's PCI DSS assessment. The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. The intent is for the assessed entity to understand which PCI DSS requirements their providers have agreed to meet.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.						
Requirement 12.9 Not Applicable – Service Providers Only						
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
12.10.1 Create the incident response plan to be implemented in the event of a system breach. Ensure the plan addresses the following, at a minimum:						The incident response plan should be thorough and contain all the key elements to allow your company to respond effectively in the event of a

PCI DSS Requirement	Method of Cardholder Data Entry to MINDBODY Services					Notes/Comments
	Direct From Consumers To MINDBODY *SAQ A*	Merchant Website Integrations *SAQ A-EP*	Merchant Entry Using Laptops and Mobile Devices *SAQ C-VT*	Card Present With Encrypted Readers *SAQ B-IP*	Card Present Legacy Readers SAQ C	
• Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.						breach that could impact cardholder data.
Requirements 12.10.2 – 12.10.6 Not Applicable						**Not Applicable for Most SAQs** As of PCI DSS 3.2.1, this requirement is applicable for merchants requiring an SAQ-D and is not required for the SAQs listed here.
Requirements 12.11 – 12.11.1 Not Applicable – Service Providers Only						