Webcor, Inc dba THE WEB Extreme Entertainment

and Web Entertainment, Inc. dba Laser Web Dayton

Information Security Policy for SAQ C Merchants

About this Document

This document contains the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton information security policies. Detailed standards and processes that support this policy are described in associated standards and procedures documentation. This document is for internal use only and is not to be distributed.

Table 1 - Revision History

Version	Date	Author	Description of Change
3.1	July, 2015	JDB	Security Policy Created

Contents

Introduction

To safeguard Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s information technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Security Policy reflects Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s commitment to comply with required standards governing the security of sensitive and confidential information.

Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton can minimize inappropriate exposures of confidential or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as the Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s information technology resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the management.

Purpose / Scope

The primary purpose of this security policy is to establish rules to ensure the protection of confidential or sensitive information and to ensure protection of Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s information technology resources. The policy assigns responsibility and provides guidelines to protect Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s systems and data against misuse or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s data network. It may apply to users of information services

operated or administered by Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton are subject to these same definitions and rules when they are using Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton‘s information technology resources.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks or data.

This security policy has been written to specifically address the security of data used by the Payment Card Industry.

Credit card data stored, processed or transmitted with Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton’s Merchant ID must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

Cardholder data within this document is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, and CVC2), Credit Card PIN, and any form of magnetic stripe data from the card (Track 1, Track 2).

Security Policy Ownership and Responsibilities

Jerome Weber is/are the assigned custodian(s) of this Security Policy. It is the responsibility of the custodian(s) of this security policy to publish and disseminate these policies to all relevant Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton system users (including vendors, contractors, and business partners). In addition, the custodian(s) must see that the security policy addresses and complies with all standards Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton is required to follow (such as the PCI DSS). This policy document will also be reviewed at least annually by the custodian(s) (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the custodian(s) listed above.

Additional Process and Standards Documents Referenced by this Security Policy

This policy document defines the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton security policies relating to the protection of sensitive data and particularly credit card data. Details on Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton standards and procedures in place to allow these policies to be followed are contained in other documents referenced by this policy. Table 2 lists other documents that accompany this security policy document, which help define Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton data security best practices.

Table 2 – Security Process and Standards Documents Referenced by Policy

Document Name	Location or Custodian
Firewall and Router Configuration Standards	Jerome Weber
System Hardening and Configuration Standards	Jerome Weber
Payment Terminal Device Review Log	Jerome Weber
Employee Computer Usage Policy	Jerome Weber
Critical Technology Device Inventory	Jerome Weber
Vulnerability Discovery and Risk Ranking	Jerome Weber
Operating Procedures	Jerome Weber
Security Awareness Training Process	Jerome Weber
SAQ C Service Provider Compliance Validation Process	Jerome Weber
Incident Response Plan	Jerome Weber
Risk Assessment Process	Jerome Weber

Build and Maintain a Secure Network and Systems

To protect sensitive or confidential data, it is critical to design and maintain a secure network infrastructure where this data can be processed and transmitted. The following polices cover the network infrastructure (hardware such as firewalls, routers, and switches) as well as requirements for the secure configuration of all system components (network hardware, servers, workstations, etc.).

1 Install and Maintain a Firewall Configuration to Protect Cardholder Data

Firewalls are devices that control computer traffic allowed between Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton's networks (internal) and untrusted networks (external). A firewall examines all network traffic and blocks those transmissions that do not meet Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton's 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 this requirement. 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.

1.2 Restrict Connections between Untrusted Network Segments and the Cardholder Data Environment

Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton will restrict connections from untrusted network segments to system components within the cardholder data environment by doing the following:

> Note: An "untrusted network" is any network that is external to the networks belonging to Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton under review, or which are out of Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton's ability to control or manage (e.g., the Internet, connected vendor networks, public wireless networks). An "untrusted network may also include a lower security Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton network that is used for normal business purposes but is not used for the storing, processing, or transmitting of sensitive data (e.g., corporate office networks).

- Maintain firewall and router configuration standards documentation[1]. (PCI-DSS Requirement 1.2)
- Firewall rules must limit all inbound and outbound traffic to/from the cardholder data network to only that which is necessary for business. (PCI-DSS Requirement 1.2.1)

1 See the Firewall and Router Configuration Standards document.

- When wireless networking is used, a firewall is required between any wireless network and the cardholder data environment. Firewall rules must prohibit insecure traffic and restrict traffic from the wireless segment to only that which is necessary for business. (PCI-DSS Requirement 1.2.3)

1.3 Prohibit Direct Public Access between the Internet and any System Component in the Cardholder Data Environment

Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton will prohibit direct public access between the Internet and any system component in the cardholder data environment by doing the following:

- A firewall is required between the cardholder data network and the Internet. (PCI-DSS Requirement 1.3.3)
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. (PCI-DSS Requirement 1.3.5)
- Use a firewall that implements stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.) (PCI-DSS Requirement 1.3.6)

2 Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton's general policy is to always change vendor-supplied defaults for system passwords or other security parameters before systems are installed in the secure network environment (cardholder data network).

Individuals with malicious intent (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.

2.1 Change Vendor Supplied Defaults

- All vendor-supplied defaults must be changed on all system components before being used in the cardholder data network. (e.g., passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts, etc.). (PCI-DSS Requirement 2.1, 2.2.d)
- If a wireless device is in use:
    - All default settings for wireless environments (equipment) connected to the cardholder data environment or transmitting cardholder data must be changed before enabling the wireless system for production use. (PCI-DSS Requirement 2.1.1.a-e)
    - The encryption keys, or passphrases, must be changed anytime anyone with knowledge of the keys leaves the companies or moves to a position that no longer requires knowledge of the keys. (PCI DSS Requirement 2.1.1.a)

- Require that all wireless devices be configured or updated to support strong encryption technologies (i.e., WPA/WPA2) for both authentication to the network and transmission of data. (PCI-DSS Requirement 2.1.1.d)

2.2 System Hardening and Standard Configuration of Devices

- Documented system configuration standards[2] must:
  - Be consistent with either SANS, ISO, NIST, CIS, or similar security industry standards and address PCI configuration requirements (e.g., password requirements, log settings, File Integrity Monitoring, Anti-virus software, etc.). (PCI-DSS Requirement 2.2)
  - Be developed that address all system components and address all known security vulnerabilities for systems used in the cardholder data network. (PCI-DSS Requirement 2.2.a)
  - Be updated as new vulnerabilities are identified. (See Section 6.1) (PCI-DSS Requirement 2.2.b)
  - Be applied when new systems used in the card network are configured and before systems are placed into production. (PCI-DSS Requirement 2.2.c)
  - Include only one primary function is implemented per server. If virtualization technologies are used, each virtual system or virtual component must have only one primary function. (PCI-DSS Requirement 2.1.d, 2.2.1)
  - Include unnecessary or insecure services, daemons, protocols are not enabled or are justified and documented as to the appropriate use of the service. (PCI-DSS Requirement 2.2.d, 2.2.2)
  - Include security parameter settings for all devices in the card network. (PCI-DSS Requirement 2.2.d)
  - Include additional security features implemented for insecure services, protocols or daemons. (PCI-DSS Requirement 2.2.d, 2.2.3)
  - Include all required functionality. These functions must support secure configuration, and only documented functionality may be present on systems in the card network. (PCI-DSS Requirement 2.2.d, 2.2.4)
  - The removal of all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers from system components in the cardholder network and document all enabled functions for each system. (PCI-DSS Requirement 2.2.d, 2.2.5)

2.3 Use Secure Protocols for Non-Console Access

- Strong cryptography must be used for any non-console or web-based management interface used for administration of systems or system components. (Use technologies such as SSH, VPN, or the latest secure versions of TLS for web-based management and other non-console administrative access.) (PCI-DSS Requirement 2.3)

2.5 Security Policies and Operational Procedures Documentation

- 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. (PCI-DSS Requirement 2.5)

2 See the System Hardening and Configuration Standards document.

Protect Cardholder Data

Cardholder data (PAN and sensitive authentication data) must not be stored electronically.

3 Protect Stored Data

Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc.

The following policies address the treatment of credit card data.

3.2 Storage of Sensitive Credit Card Authentication Data

- Never store sensitive cardholder data such as the authentication data (Track, CVC, and PIN) after an authorization event has taken place (even if encrypted). (PCI-DSS Requirement 3.2.d).
- All sensitive authentication data must be deleted or rendered unrecoverable upon completion of the authorization process. (PCI-DSS Requirement 3.2.c)
- Never store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere) in any database, log file, debug file, etc. after any type of card authorization event. (PCI-DSS Requirement 3.2.1).
- Never store the Card Validation Code (CVC) data (3- or 4-digit number located on the back or front of the credit card) in any database, log file, and debug file, etc. after any type of card authorization event. (PCI-DSS Requirement 3.2.2).
- Never store the cardholders Personal Identification Number (PIN) data (includes actual PIN number or Encrypted PIN block obtained during a debit card transaction from the PIN Entry Device) in any database, log file, debug file, etc. after any type of card authorization event. (PCI-DSS Requirement 3.2.3).

3.3 Mask Credit Card Numbers in Displays Wherever Possible

- Credit card PAN Data will be masked or truncated when displaying card numbers on any media and/or payment terminal. (PCI-DSS Requirement 3.3)

4 Encrypt Transmission of Cardholder Data across Open, Public Networks

Cardholder data 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.

4.1 Transmission of Card Data over Public Networks

- Strong encryption algorithms and protocols (i.e., TLS, IPSEC, SSH) must be used whenever cardholder data is transmitted or received over open, public networks. The following controls must be part of the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton data transmission policies: (PCI-DSS Requirement 4.1.a)
    - Only trusted keys or certificates will be accepted. (PCI-DSS Requirement 4.1.b)
    - The data transmission protocol must be implemented to use only secure protocol configurations, and must not support insecure versions or configurations (e.g., use the latest secure TLS and SSH versions only). (PCI-DSS Requirement 4.1.c)

- The encryption strength is appropriate for the encryption methodology in use. (PCI-DSS Requirement 4.1.d)
- For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (PCI-DSS Requirement 4.1.e)
- If SSL or early TLS is used on a POS POI terminal, documentation must be created detailing how it was verified that the terminal is not susceptible to any known exploits for SSL or early versions of TLS. Documentation must include evidence (vendor documentation, system/network configuration details, etc). (PCI-DSS Requirement 4.1.f)
- If SSL or early TLS is used anywhere but a POS POI terminal, a risk mitigation and migration plan must be created, which includes the following: (PCI DSS Requirement 4.1.g)
  - Description of how it is used, including what data is being transmitted, the types and number of systems that use and/or support SSL or early TLS and the type of environment.
  - The risk assessment results, including the risk reduction controls that are in place.
  - A process of how new vulnerabilities associated with SSL and early TLS are monitored.
  - A description of change control processes that are in place to ensure no new environments are created which utilize SSL and/or early TLS.
  - An overview of the migration project plan that includes a migration completion date no later than June 30th, 2016.
- If wireless networks transmitting cardholder data or connected to the cardholder data environment are in use, a documented standard must be created which ensures the use of strong encryption and industry best practices. (PCI-DSS Requirement 4.1.1)

4.2 Transmission of Card Data via End User Messaging Technologies

- It is prohibited to transmit cardholder data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (PCI-DSS Requirement 4.2)

Maintain a Vulnerability Management Program

System components within the cardholder data network must be part of an active vulnerability maintenance program. This program will control the existence of malicious software (e.g., anti-virus software) and provide policies covering development efforts and system or software updates/upgrades such that security is maintained.

The following policies ensure system components are protected from malicious software and vulnerabilities that result from software bugs and improperly patched applications and operating systems.

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 a sensitive network segment during many business approved activities, including employees’ 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.

5.1 Deploy anti-virus software to protect systems

- Anti-virus software must be deployed on all systems in the card network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the cardholder network segment. (PCI-DSS Requirement 5.1)
- Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.). (PCI-DSS Requirement 5.1.1)
- For systems considered not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue not to require anti-virus software. (PCI-DSS Requirement 5.1.2)

5.2 Ensure that all anti-virus mechanisms are current

- All anti-virus software and its associated definition files must be kept up-to-date at all times. (PCI-DSS Requirement 5.2.a)
- All anti-virus software must be actively running, configured to perform automatic updates, and set to run periodic scans. (PCI-DSS Requirement 5.2.b)
- Anti-virus software must be capable of generating audit logs and audit logs must be retained for one year. (PCI-DSS Requirement 5.2.c)

5.3 Ensure that all anti-virus mechanisms are actively running

- All anti-virus software installations and configurations must be actively running at all times. (PCI-DSS Requirement 5.3.)
- Anti-virus configurations do not allow users to disable or alter the software unless specifically authorized by management on a case-by-case basis for a limited time. (PCI-DSS Requirement 5.3)

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 that must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

6.1 Vulnerability risk ranking process

- System administrators are to subscribe to outside sources for security vulnerability information and system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include SecurityFocus, A/V companies, SANS, CIS, Secunia, Microsoft, etc. (PCI-DSS Requirement 6.1)
- When any vulnerability (or potential vulnerability) is found using the documented vulnerability discovery and risk ranking process[3], it must be evaluated and assigned a ranking based on the risk level. At a minimum, the highest risk vulnerabilities should be assigned a “High” risk ranking. (PCI-DSS Requirement 6.1)

3 See the Vulnerability Discovery and Risk Ranking Process document.

6.2 Regularly update systems and software

- All system components and software must have the latest vendor-supplied security patches installed. (PCI-DSS Requirement 6.2.a)
- All critical system and software patches must be installed within 30 days of vendor release. (PCI-DSS Requirement 6.2.b)

Implement Strong Access Control Measures

Access to system components and software within the sensitive data environment (cardholder data network) must be controlled and restricted to those with a business need for that access. This is achieved with active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

7 Restrict Access to Cardholder Data by Business Need to Know

Systems and processes must be in place to limit access to critical data and systems based on an individuals need to know and according to job responsibilities.

"Need to know" is when access rights are granted to the least amount of data and privileges needed to perform a job.

7.1 Restrict Access to Cardholder Data and Systems in Cardholder Data Environment

- Access to cardholder data and system components must be restricted to only those individuals whose job requires such access. (PCI-DSS Requirement 7.1)
- Restrict access to privileged user IDs to the least privileges necessary to perform job responsibilities and assigned to only those roles that specifically require the privileged access. (PCI-DSS Requirement 7.1.2)
- Access assigned to individual personnel is based on their job classification and function. (PCI-DSS Requirement 7.1.3)

8 Identify and Authenticate Access to System Components

It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.1 Vendor Access

- Manage IDs used by vendors to access, support, or maintain system components via remote access, ensuring that they are only enabled for the time period needed, disabled when not in use and they are monitored by Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton employees during use. (PCI-DSS Requirement 8.1.5a-b)

8.3 Two-factor Authentication

- Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance). (PCI-DSS Requirement 8.3)

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.

It is the policy of Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton that no full cardholder data (credit card numbers) shall be stored in any format (electronic or hardcopy media). If sensitive cardholder data is ever discovered or received, management must be notified and it shall be immediately destroyed, redacted, or truncated following the information in section 9.8 of this policy. (PCI-DSS Requirement 9.8)

9.1 Limits and Monitor Physical Access to Systems

- Restrict access to network jacks by implementing physical and/or logical controls. (PCI-DSS Requirement 9.1.2)

9.8 Media Destruction Policies and Procedures

- Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. (PCI-DSS Requirement 9.8)
- It is the policy of Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton that cardholder data that is identified to be past expiration or has no business justification to retain must be properly destroyed. Techniques for data destruction vary depending on type of media and are defined as follows: (PCI-DSS Requirement 9.8.1.a)
    - Electronic media (hard drives, flash drives, etc.) containing cardholder data must be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or the media must be physically destroyed. (PCI-DSS Requirement 9.8)
    - Hardcopy media (faxes, printed documents and reports, etc.) must be crosscut shredded, pulped, or incinerated according to industry-accepted standards.
- If applicable, all containers used to store media containing cardholder data to be destroyed must be locked and in a secure area at all times. Such containers are only to be given to authorized personnel or third parties for the purpose of destruction. (PCI DSS Requirement 9.8.1.b)

9.9 Protection from Tampering and Substitution

- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. (PCI-DSS Requirement 9.9)
- Maintain an up to date list of devices that includes the following: (PCI-DSS Requirement 9.9.1/See Payment Terminal Device Review Log in Table 2)
    - Make and model of the device

- Location of the device
- Device Serial number or other method of unique identification.

- Periodically inspect device surfaces to detect tampering (for example, 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). (PCI-DSS Requirement 9.9.2)
- Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI-DSS Requirement 9.9.3)
  - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to 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).

Regularly Monitor and Test Networks

Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The following policies address system monitoring and vulnerability testing.

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 without system activity logs. Detailed monitoring procedures should be developed and documented to meet the following policies.

10.2 Generation of Audit Trails

- Implement automated audit trails for all system components to capture the following events: (PCI-DSS Requirement 10.2)
  - All actions taken by any individual with root or administrative privileges.(PCI-DSS Requirement 10.2.2)
  - Invalid logical access attempts. (PCI-DSS Requirement 10.2.4)
  - 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. (PCI-DSS Requirement 10.2.5)

10.3 Audit Trail Entries

- Record at least the following audit trail entries for all system components for each event: (PCI-DSS Requirement 10.3)
  - User Identification. (PCI DSS Requirement 10.3.1)
  - Type of event. (PCI DSS Requirement 10.3.2)

- Date and Time. (PCI DSS Requirement 10.3.3)
- Success or failure indication. (PCI DSS Requirement 10.3.4)
- Origination of event. (PCI DSS Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI DSS Requirement 10.3.6)

10.6 Log Review

- Review logs and security events for all system components to identify anomalies or suspicious activity by performing the following: (PCI-DSS Requirement 10.6)
  - Review the following at least daily: (PCI DSS Requirement 10.6.1)
    - All security events.
    - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could affect the security of 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.).
- 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.[4] (PCI DSS Requirement 10.6.2)
- Follow up exceptions and anomalies identified during the review process. (PCI DSS Requirement 10.6.3)

10.7 Audit Trail History

- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from backup). (PCI-DSS Requirement 10.7)

10.8 Security Policies and Operational Procedures Documentation

- 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. (PCI-DSS Requirement 10.8)

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 must be tested frequently to ensure security controls continue to reflect a changing environment. Detailed testing procedures[5] should be developed and documented to meet the following policies.

4 See the Risk Assessment document.

5 See the Operating Procedures document.

11.1 Rogue Wireless Network Detection

- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton will have a documented process[6] that will be used at least quarterly to detect unauthorized wireless networks/devices within the card-processing environment. (PCI-DSS Requirement 11.1 and 11.1.2)
- Process defined will address the detection and identification of multiple types of wireless devices such as WLAN cards inserted into system components, portable wireless devices connected to system components, or wireless devices connected to a network port or network device. (PCI-DSS Requirement 11.1)
- Any automated wireless monitoring solution must generate alerts if rogue devices are detected. Process documentation must define a response procedure if rogue devices are found.
- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton will maintain an inventory of all authorized wireless access points including a documented business justification. (PCI-DSS Requirement 11.1.1)
- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton will define incident response procedures (see PCI-DSS Requirement 12.10) in the event an unauthorized wireless access point is detected (PCI-DSS Requirement 11.1.2)

11.2 Vulnerability Assessment Scans

- Internal and external vulnerability assessment scans must be performed at least quarterly and after any significant change in the cardholder data network (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). (PCI-DSS Requirement 11.2)
- Internal vulnerability scans must be: (PCI-DSS Requirement 11.2.1.a-c)
    - Performed quarterly.
    - Be performed by a qualified internal resource with organizational independence or a qualified external third party.
    - Have a process to include a rescan until all “high-risk” vulnerabilities (as defined in PCI-DSS Requirement 6.1) are resolved. (PCI DSS Requirement 11.2.3.b)
- External vulnerability scans must (PCI-DSS Requirement 11.2.2.a-c)
    - Be performed quarterly.
    - Be performed by an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) with rescans until passing scans are achieved.
    - Contain no vulnerabilities that are scored 4.0 or higher by the CVSS.
    - Run on all external IP addresses that could be used to gain access to the cardholder data environment. (PCI-DSS Requirement 11.2)
- Internal and external scans per the above policies are required quarterly and after any change deemed to be significant. (PCI DSS Requirement 11.2.3)
- Ensure that results of each quarter’s internal and external vulnerability assessments are to be documented and retained for review. (PCI-DSS Requirement 11.2)

6 See the Operating Procedures document.

11.3 Penetration Testing

- If segmentation is used to isolate the CDE from other networks, a segmentation test is required to confirm all methods of segmentation are effective in isolating the CDE from out-of-scope systems or networks. These tests must be documented and performed at least annually and after any changes to segmentation controls or methods. (PCI DSS Requirement 11.3.4)

11.5 Change Detection

- Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. (PCI-DSS Requirement 11.5)
- A process is in place describing how to respond to alerts generated by the change-detection mechanism. (PCI-DSS Requirement 11.5.1)

Maintain an Information Security Policy

Without strong security policies and procedures, many of the layers of security controls become ineffective at preventing data breach. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton security policies described in this document.

12 Maintain a Security Policy that Addresses Information Security for All Personnel

A strong security policy sets the security tone for Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.

> Note: “Employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the company’s site.

12.1 Publish, Distribute, and Update the Information Security Policy

- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI-DSS Requirement 12.1)
- The Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (PCI-DSS Requirement 12.1.1)

12.3 Critical Technology Usage Policies

- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton must develop usage policies for all critical technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants

(PDAs), e-mail usage and Internet usage), and define proper use of these technologies. (PCI-DSS Requirement 12.3)[7]

- Explicit management approval is required prior to using the technologies. (PCI-DSS Requirement 12.3.1)
- Any use of the technology must be authenticated with a user ID and password or other authentication item (for example, token). (PCI-DSS Requirement 12.3.2)
- A list must be maintained of all such devices in use and contain the personnel authorized to use them.[8] (PCI-DSS Requirement 12.3.3)
- Acceptable uses for the technology must be defined and documented. (PCI-DSS Requirement 12.3.5)
- Acceptable network locations for the technologies must be defined and documented. (PCI-DSS Requirement 12.3.6)
- Remote-access technologies in use must automatically disconnect sessions after a specific period of inactivity. (PCI-DSS Requirement 12.3.8)
- Only activate remote-access technologies for vendors and business partners only when needed and immediately deactivate remote-access sessions after use. (PCI-DSS Requirement 12.3.9)

12.4 Assign Information Security Responsibilities and Train Employees

- The Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton's information security policy and procedures apply to all employees (full, part-time, or work study employees), contractors, and individuals providing services for Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton and could affect security of cardholder information. (PCI-DSS Requirement 12.4)

12.5 Assign Information Security Management

- The overall responsibility of information security at *Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton* falls under the office of Jerome Weber (PCI-DSS Requirement 12.5)
- Specifically the following responsibilities must be assigned: (see form in Appendix A)
    - Establishing detailed documentation of security incident response and escalation procedures and distributing these procedures. (PCI-DSS Requirement 12.5.3)

12.6 Security Awareness Program

- A formal security awareness program[9] must exist and participation is required for all employees working within the cardholder data environment. (PCI-DSS Requirement 12.6.a)

12.8 Policies for Sharing Data with Service Providers

- In order to conform to industry best practices, it is required that due diligence is performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on Webcor, Inc dba THE WEB Extreme Entertainment

7 See the Employee Computer Usage Policy document

8 See the Critical Technology Device Inventory

9 See the Security Awareness Training Process document.

and Web Entertainment, Inc. dba Laser Web Dayton's behalf. Service providers, which could affect the security of sensitive cardholder data, are also in-scope of this policy.

- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton shall maintain a documented list of all applicable service providers in use. (PCI-DSS Requirement 12.8.1)
- A written agreement with all applicable service providers is required and must include an acknowledgement of the service providers' responsibility for securing all cardholder data they receive from or on behalf of Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton, or to the extent that they could affect the security of a cardholder data environment (PCI-DSS Requirement 12.8.2). In addition, the service provider must agree to provide compliance validation evidence on an annual basis. (PCI-DSS Requirement 12.8.4). Prior to engaging with an applicable service provider, a thorough due diligence process as prescribed in the above referenced Service Provider Compliance Validation Process document in table 2. (PCI-DSS Requirement 12.8.3)
- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton shall annually review evidence provided by applicable service providers demonstrating their continuing PCI DSS compliance. (PCI-DSS Requirement 12.8.4)
- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton shall maintain a list of which PCI DSS requirements are managed by each service provider, and which are managed by Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton. (PCI-DSS Requirement 12.8.5)

12.10 Incident Response Plan Policies

Incidents or suspected incidents regarding the security of the cardholder data network or cardholder data itself must be handled quickly and in a controlled, coordinated and specific manner. An incident response plan must be developed and followed in the event of a breach or suspected breach. The following policies specifically address the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton incident response plan[10]:

- Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton must maintain a documented incident response plan (IRP) and be prepared to respond immediately to a system breach. (PCI-DSS Requirement 12.10)
- The IRP must clearly define roles and responsibilities for response team members. (PCI-DSS Requirement 12.10.1)
- The IRP must define communication strategies to be used in the event of a compromise including notification of payment brands. (PCI-DSS Requirement 12.10.1)
- The IRP must define specific incident response procedures to be followed. (PCI-DSS Requirement 12.10.1)
- The IRP must document business recovery and continuity procedures. (PCI-DSS Requirement 12.10.1)
- The IRP must detail all data back-up processes. (PCI-DSS Requirement 12.10.1)

10 See the Incident Response Plan document.

- The IRP must contain an analysis of all legal requirements for reporting compromises of sensitive data (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise of California resident's data). (PCI-DSS Requirement 12.10.1)
- The IRP must address coverage and responses for all critical system components. (PCI-DSS Requirement 12.10.1)
- The IRP must include or reference the specific incident response procedures from the payment brands. (PCI-DSS Requirement 12.10.1)

Appendix A – Management Roles and Responsibilities

Assignment of Management Roles and Responsibilities for Security

As required by policy in Section 12.5 of this security policy, the following table contains the assignment of management roles for security processes.

Management Security Responsibilities

Name of Role , Group, or Department	Date Assigned	Description of Responsibility
Jerome Weber	5/12/2016	Establish, document, and distribute security policies
Jerome Weber	5/12/2016	Monitor, analyze, and distribute security alerts and information
Jerome Weber	5/12/2016	Establish, document, and distribute security incident response and escalation policies
Jerome Weber	5/12/2016	Administration of user accounts on systems in the cardholder data network
Jerome Weber	5/12/2016	Monitor and control all access to cardholder data

Appendix B – Agreement to Comply

Agreement to Comply with Information Security Policies

All employees working with sensitive cardholder data must submit a signed paper copy of this form. Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton management will not accept modifications to the terms and conditions of this agreement.

_____

Employee's Printed Name

_____

Employee's Department

_____

Employee's Telephone Number

_____

Employee's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton internal information, or information that has been entrusted to Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton, I agree to return to Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton all information to which I have had access because of my position with Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton manager who is the designated information Owner.

I have access to a copy of the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton Information Security Policies Manual, I have read and understand the manual, and I understand how it affects my job. As a condition of continued employment at Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the Webcor, Inc dba THE WEB Extreme Entertainment and Web Entertainment, Inc. dba Laser Web Dayton Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree that I will promptly report all violations or suspected violations of information security policies to Jerome Weber.

_____

Employee's Signature