Introduction

Threats can be introduced to Chaminade’s environment simply by connecting a third-party without efficient security practices and controls in place. Should an attacker penetrate the third-party’s network, they may route their way via the connected third-party into Chaminade’s network. In some cases, third-parties have privileged access (meaning they have direct access to cardholder data in the production environment), thus gaining unauthorized access to the cardholder data environment. Chaminade’s cardholder data environment includes all systems, applications, equipment, individuals, locations, and connections used for, and involved with, the transmittal, processing, and/or storage of cardholder data.

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

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

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

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

Scope

This policy applies to Chaminade employees, third-parties, service providers, contractors, temporary employees, and/or other staff members at Chaminade with responsibilities for maintenance and management of the cardholder data environment at Chaminade, whether conducting activities on Chaminade premises or off-site.

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

Distribution

This policy is to be distributed to all those with responsibilities for maintenance and management of the cardholder data environment at Chaminade, to include Chaminade employees, third-parties, service providers, contractors, temporary employees, and/or other staff members.

The most current version of this policy is to be readily available and accessible from the Chaminade portal under Administration -> Policy Manuals.

Exceptions

There are currently no exceptions to this policy. Requests for exceptions may be submitted to the Dean of Information Services for review and approval using email.

Violations

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

Review Schedule

The next scheduled review date is December 1, 2013 by the Dean of Information Services, to be approved by the Dean of Information Services and Executive Director for Compliance and Personnel.
Policy

Assessment of Risk

Third-parties must be given a risk assessment prior to being connected to the Chaminade cardholder data environment. No third-party may be connected to the Chaminade environment prior to receiving this assessment. Should a third-party have not received this risk assessment and is currently connected, the risk assessment is to be performed before they may be reconnected. This assessment is to include discovery of threats that may lead to potential vulnerabilities, and a review of any support contract.

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

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

Network Diagram

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

List of Third-Parties

Chaminade is to maintain a current list of connected third-parties with details of whether they have direct access to the cardholder data environment. This is to clearly denote which third-parties have privileged access and so special attention may be paid to them during session monitoring. The list of third-parties is to also include their PCI compliance status and date of, whether they have accepted by their acquiring bank or VISA or have performed a SAQ (whichever is applicable to their Level as defined above).

PCI Compliance Status

The status of connected third-parties achieving PCI compliance is to be reviewed annually. All third-parties with direct access to the cardholder data environment must obtain PCI compliance or have an official exception provided by their acquiring bank or VISA. Should a third-party with privileged access not have obtained this compliance status, they are to document in writing their efforts in doing so with the target completion date. Chaminade is to monitor the compliance efforts of these third-parties.
Terms and Conditions

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

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

- Protect Chaminade’s cardholder data and environment.
- Follow Chaminade’s policies and procedures at all times, unless there is specific approval from the Dean of Information Services.
- Use only Chaminade-approved security controls and practices.
- Communicate any suspected compromise of third-party systems connected to Chaminade’s cardholder data environment.
- Escalate suspected breaches and incidents to the Chaminade within 8 business hours.
- Retain and dispose of electronic and paper cardholder data media in a secure manner.
- Comply with federal and industry laws and regulations.
- Train individuals with access to Chaminade systems and data on effective safeguard measures.
- Maintain security awareness amongst personnel.
- Conduct criminal background checks on all individuals with access to Chaminade’s network, systems, and data. Background checks are to be performed prior to granting individuals access.
- Removing access permissions immediately upon termination of the individual.
- Maintaining appropriate access control methods, including two-factor remote access.
- Only attempting to connect to Chaminade’s cardholder data environment during authorized periods, and disconnecting when the work is completed.
- Permitting Chaminade to perform periodic reviews, and forensic investigations upon the Dean of Information Services’ determination.
- Physically and logically segregating Chaminade systems, networks, and data from those belonging to any other clients.
- Implementing logging and audit trail requirements.
- Notifying and obtaining agreement from Chaminade prior to outsourcing work to other third-parties.

Change Management

Any changes made by the third-party in regards to their security controls and practices as well as organizational process changes must be communicated to Chaminade. Chaminade is to review the change as to its potential impact on Chaminade. This is to help protect against the possibility of inadvertently introducing open avenues for attack. Once the review has been performed, the change documentation and description of any residual risk from the third-party performing the change is to be reviewed and accepted by the Dean of Information Services.

The Third Party Change Documents must be used to track changes from their initial request stage through review to documentation of residual risk to approval by the Dean of Information Services.
Any system or application changes with impact on Chaminade are to be tested by the third-party in a test environment prior to being placed into the production environment.

**Event Management and Response**

Logs for Chaminade systems, applications, and equipment managed by the third-parties are to be generated, reviewed, and maintained to provide an audit trail. Logs are to be synced to a safeguarded central location.

Incidents, whether suspected or actual, are to be reported to Chaminade within 8 business hours so they may be responded to in accordance with the Incident Response Plan. Determination of the third-party’s role in incident response and containment should be clearly defined.

**Security Awareness**

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

**Background Checks**

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

**Access Controls**

Access to the Chaminade’s cardholder data environment is to be limited to only those individuals with a business need-to-know. Individual authentication, meaning a unique userID and unique password, is to be used.

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

Password management is, where feasible, to follow the password requirements for other institutional systems.

**Monitoring and Managing Third-Party Access**

Third-party access may only be permitted with prior authorization from the Director of Business Services, and is to be connected immediately after use. The Director of Business Services or a designated proxy are to monitor the access at all times. In some cases, access is granted to third-parties on a 24/7/365 basis. These types of access should be approved by the Dean of Information Services prior to access being granted, and Director of Networking and Systems is to periodically monitor the connection without prior notification to the third-party.
The third-party may not attempt to access Chaminade’s cardholder data environment without prior authorization at anytime, and doing so may result in the initiation of the incident response plan.

**Segregation**

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