Router Configuration and Management Policy

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change/s</th>
<th>Author/s</th>
<th>Approver/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01/01/2013</td>
<td>Initial written policy.</td>
<td>Kyle Johnson</td>
<td>Dean of Information Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Executive Director for Compliance and Personnel Services</td>
</tr>
</tbody>
</table>

Introduction

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

Routers route traffic will be based upon internal addresses and defined route tables to ensure that it arrives at its intended destination. Routers may also assist with functions performed by the firewall(s) where certain data packets are blocked. Subsequently, the protection of the router and of its configuration file is important in order to protect against external traffic being transmitted into trusted environments that contain systems which transmit, process, and/or store cardholder data, and the internal network in general.

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

Purpose

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

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

Placement

Trusted environments include known zones that contain systems that transmit, process, and/or store cardholder data, and the internal network in general. Untrusted environments include internet-facing access points, unknown environments, wireless networks, and zones that do not contain such systems that transmit, process, and/or store cardholder data.

Configuration Services

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

Router files are to be documented and kept current, and reviewed by the Director of Networking and Systems on a semi-annual basis, at a minimum. The Director of Networking and Systems must document the review and results in the Router Review Log. The Dean of Information Services is to review and sign-off on the findings. Exceptions are to be submitted following the Exceptions process noted earlier in this Policy.

Change Management

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

The Firewall/Router Change Documents must be used to track changes from initial request stage through the review of documentation of residual risk to approval by the Dean of Information Services.

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

Synchronization of Router Files

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

Access Controls

Access to the routers should be limited to only those individuals with a business need-to-know. Individual authentication (a unique userID and unique password) is to be used by the administrators, unless the Dean of Information Services has specifically approved an Admin account.
Remote access to the routers may only be performed using a secure network protocol, such as SSH, and users must use two-factor authentication (the user must possess something they have and something they know in addition to their userID).

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

**Event Management and Response**

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

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

**Time Synchronization**

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

**Logical Management of Network Components**

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

- **Configuration and maintenance of router files**: Director of Networking and Systems
- **Installation of routers**: Director of Networking and Systems
- **Deployment of routers**: Director of Networking and Systems
- **Network diagram maintenance**: Director of Networking and Systems
- **Reviews of router config file change requests**: Director of Networking and Systems
- **Approvals of router config file change requests**: Dean of Information Services