



## **IT 17.05: Router Management Standards**

<b>Policy Authority</b>	BTS Administrative Rule 1.03- Ownership of Information Technology Assets BTS Administrative Rule 2.01- Security Administrative Rule
<b>Purpose</b>	Routers and switches provide the primary network mechanism for forwarding traffic across the City's network. These devices require periodic review and maintenance to mitigate the threats associated with unauthorized network traffic.
<b>Policy</b>	Regular reviews of City routers and switches shall take place in accordance with PCI-DSS (Payment Card Industry- Data Security Standard) and industry best practice.
<b>Procedure</b>	In order to accomplish the aforementioned policy, certain router management procedures must be established including: <ul style="list-style-type: none"><li>• Scope</li><li>• Roles and Responsibilities</li><li>• Schedule &amp; Process</li></ul>

### **Scope**

Routers, switches, and any other network device that are in scope of Payment Card Industry- Data Security Standard (PCI-DSS).

### **Roles and Responsibilities**

There are two groups, Network Engineering and Information Security, involved in evaluating and implementing a PCI-DSS compliant environment within the City's network devices. Their roles and responsibilities are described below:

**Network Engineering-** Network Engineering reviews all PCI-DSS network devices to ensure that their configuration and rule set provides a secure environment that transmits only traffic with documented needs. Network Engineering is responsible for retaining an in depth knowledge of the City's network architecture and configuration. Network Engineering implements Information Security approved rule changes, patches, or firmware upgrades.

**Information Security-** the Information Security Office provides policy guidance on PCI-DSS standards; particularly as it relates to router configuration and rule sets. Information Security provides additional assistance to Network Engineering when questions arise related to the interpretation of PCI-DSS scope and compliance.

### **Schedule & Process**

#### **Schedule**

Network Engineering holds semi-annual reviews of PCI-DSS network devices. These reviews include necessary Network Engineering staff and a representative from Information Security.

**Process**

Network Engineering shall maintain electronic records that document the meeting minutes and any remediation actions to be taken.

In these meetings, the following review takes place:

- 1) A review of the current list of PCI-DSS devices to ensure its completeness and accuracy.
- 2) A review of the current network device configuration(s) to ensure that the current and start-up configurations match.
- 3) A review of the current software versions to ensure that they are current.
- 4) A review of any router rules to ensure their business necessity.

**Revision History**

Version	Effective Date	Authored By	Approved By	Date
1.0	3/31/09	Logan Kleier, Information Security Manager	BTS Leadership Team	3/13/09