

## ITSec 1: FIREWALL CONFIGURATION POLICY

Responsible Business Unit: IT  
Affected Business Unit: All  
Created by: Chris Pofahl

Creation Date: 1/03/2017  
Effective Date: 3/2/2017  
Expiration Date: [Expiration Date]

### Introduction

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.

### Purpose

Requirement 1 of PCI DSS requires 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.

### Scope

#### 1. Policy Justification

- a. This Policy related document
- b. Additionally, this Policy related document insures the integrity, availability, and security of the City of Waukesha's digital assets.

#### 2. Affected Staff

- a. All City departments, offices, divisions, and agencies
- b. All represented and non-represented employees, contractors, and temporary workers

#### 3. Significantly Related Documents and Policies

- a. ITFW-0.1 FIREWALL CONFIGURATION POLICY
- b. ITPW-0.1 SYSTEM AND PASSWORD POLICY
- c. ITSSD-0.1 STORING SENSITIVE DATA POLICY
- d. ITTSD-0.1 TRANSMISSION OF SENSITIVE DATA POLICY
- e. ITAV-0.1 ANTIVIRUS POLICY
- f. ITVS-0.1 VULNERABILITY SCANNING POLICY

#### 4. Policy Maintenance

- a. Review this policy annually by Information Technology Board

#### 5. Policy Statement

- a. A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- b. A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- c. Firewall and router configurations must restrict connections between untrusted networks and any systems in the card holder data environment.
- d. Stateful Firewall technology must be implemented where the Internet enters the City of Waukesha Card network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- e. All inbound and outbound traffic must be restricted to that which is required for the card holder data environment.
- f. All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- g. All outbound traffic has to be authorized by management (i.e. what are the whitelisted category of sites that can be visited by the employees) and the restrictions have to be documented
- h. The City of Waukesha will have firewalls between any wireless networks and the cardholder data environment.
- i. Disclosure of private IP addresses to external entities must be authorized.
- j. A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.
- k. The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- l. No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

## 6. Enforcement

- a. Process Violation – See City of Waukesha HR Policy *B20 - Software Usage and Standardization* approved this 2nd day of February 2010.
- b. Additionally, see related regulation (governance, security, regulatory, HIPAA, SOX, ITIL, ISO, COBIT, PCI DSS, Homeland Security, State of Wisconsin, Federal Government, etc.) as applicable. **U.S. State Breach Notification Laws, U.S. State Social Security Number Confidentiality Laws, U.S. Patriot Act, U.S. Federal Trade Commission (FTC) Consumer Rules, U.S. Health Insurance Act (HIPAA).**

## 7. Standards Supporting this Policy

- a. PCI DSS
- b. **U.S. State Breach Notification Laws**
- c. **U.S. State Social Security Number Confidentiality Laws**
- d. **U.S. Patriot Act**

- e. **U.S. Federal Trade Commission (FTC) Consumer Rules**
  - f. **U.S. Health Insurance Act (HIPAA).**
- 8. Procedures Enforcing this Policy**

## Approval

The Person(s) listed below approve this ITFW-0.1 FIREWALL CONFIGURATION POLICY Approval guideline for IT use on the date specified.

**Approver Name**

[Approved by]

**Approved On**

[Approved]

