ITSec 6: VULNERABILITY MANAGEMENT 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

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which 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.

Purpose

Requirement 6 of PCI DSS calls for businesses to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. This Policy Document addresses the vulnerability scanning by a 3rd party section of the Vulnerability Management Program requirements of PCI DSS. **Additionally, vulnerability scanning helps identify any exploitable vulnerabilities. By remediating these vulnerabilities the City can be better protected against breaches, or attacks and prevent sensitive data loss that includes, but is not limited to Bank Account and routing numbers, Medical Terms and Personal Identifiable Information (PII), should be handled in the same manner as card holder data. PII includes, but is not limited to U.S. Individual Taxpayer Identification Number (ITIN),U.S. Social Security Number (SSN),U.S. / U.K. Passport Number, U.S. Driver's License Number, U.S. Social Security Number (SSN).**

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. ITAV-0.1 ANTIVIRUS POLICY

b. ITFW-0.1 FIREWALL CONFIGURATION POLICY
c. ITPW-0.1 SYSTEM AND PASSWORD POLICY
d. ITCHD-0.1 STORING CARD HOLDER DATA POLICY

4. **Policy Maintenance**
   a. Review this policy annually by Information Technology Board
5. **Policy Statement**
   a. All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
   b. As part of the PCI-DSS Compliance requirements, the City of Waukesha will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
   c. Quarterly internal vulnerability scans must be performed by the City of Waukesha by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
   d. Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the Company's internal staff. The scan process should include re-scans until passing results are obtained.
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 ITSec 6: VULNERABILITY MANAGEMENT POLICY
Approval guideline for IT use on the date specified.

Approver Name	**Approved On**
[Approved by]	[Approved]