ITSec 2: SYSTEM AND PASSWORD POLICY

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

Creation Date: 5/17/2018
Effective Date: 6/19/2018
Expiration Date: [Expiration Date]

Introduction

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Purpose

Requirement 2 of PCI DSS requires all users, including contractors and vendors with access to the City of Waukesha systems to secure their passwords.

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. ITSec 1: FIREWALL CONFIGURATION POLICY
    b. ITSec 2: SYSTEM AND PASSWORD POLICY
    c. ITSec 3: STORING SENSITIVE DATA POLICY
    d. ITSec 4: TRANSMISSION OF SENSITIVE DATA POLICY
    e. ITSec 5: ANTIVIRUS POLICY
    f. ITSec 6: VULNERABILITY MANAGEMENT POLICY
    g. ITSec 7: ACCESS TO SENSITIVE DATA POLICY
    h. ITSec 8: USER ACCESS AND AUTHENTICATION POLICY
    i. ITSec 9: PHYSICAL ACCESS TO SENSITIVE DATA POLICY
    j. ITSec 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA
    k. ITSec 11: TESTING SECURITY SYSTEMS AND PROCESSES POLICY
    l. ITSec 12: MAINTING AN INFORMATION SECURITY POLICY

m. ITSec 13: SECUTIY AWARENESS TRAINING POLICY
n. ITSec 14: DISPOSING OF SENSITIVE DATA POLICY

4. Policy Maintenance

a. Review this policy annually by Information Technology Board

5. Policy Statement

a. A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO).
b. System configurations should be updated as new issues are identified (as defined in PCI DSS requirement 6.1).
c. System configurations must include common security parameter settings.
d. The systems configuration standard should be applied to any new systems configured.
e. All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into the City of Waukesha network and all unnecessary services and user/system accounts have to be disabled.
f. All unnecessary default accounts must be removed or disabled before installing a system on the network.
g. Security parameter settings must be set appropriately on System components
h. All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
i. All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
j. Any insecure protocols, daemons, services in use must be documented and justified.
k. All users with access to card holder data must have a unique ID.
l. All user ID's for terminated users must be deactivated or removed immediately.
m. The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
n. All system and user level passwords must be changed on at least a quarterly basis.
o. A minimum password history of four must be implemented.
p. A unique password must be setup for new users and the users prompted to change the password on first login.
q. Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
r. Where SNMP is used, the community strings must be defined as something other than the default.
s. Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.

t. All non-console administrative access will use appropriate technologies like ssh,vpn etc or strong encryption is invoked before the administrator password is requested
u. System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands
v. Administrator access to web based management interfaces is encrypted using strong cryptography.
w. All users must use a strong password to access the company network or any other electronic resources. A strong password must:
    i. Be as long as possible (never shorter than 8 characters).
    ii. Include mixed-case letters,
    iii. Include digits and punctuation marks, if possible.
    iv. Not be based on any personal information.
    v. Not be based on any dictionary word, in any language.

x. Workstations must be physically secured. If an operating system without security features is used (such as Linux, Windows, or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
y. To protect against network analysis attacks, both the workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

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 2: SYSTEM AND PASSWORD POLICY

Approval guideline for IT use on the date specified.

Approver Name	Approved On
[Approved by]	[Approved]