ITSec 8: USER ACCESS AND AUTHENTICATION POLICY

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

Creation Date: 5/17/2018
Effective Date: 7/3/2018
Expiration Date: [Expiration Date]

Introduction

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

Purpose

Requirement 8 of PCI DSS requires that each user have a unique ID before accessing any systems for cardholder data. This policy has been broadened to include users password requirements, when multi factor authentication should be used, and how to handle inactive

By following this policy 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. 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. Assign all users a unique ID before allowing them to access system components or cardholder data.
b. Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
c. Immediately revoke access for any terminated users.
d. Remove/disable inactive user accounts within 90 days.
e. Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:
    i. Enabled only during the period needed, and disabled when not in use.
    ii. Monitored when in use.
f. Limit repeated access attempts by locking out the user ID after not more than five attempts.
g. Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
h. If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
i. In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:
    i. Something you know, such as a password or passphrase
    ii. Something you have, such as a token device or smart card
    iii. Something you are, such as a biometric.
j. Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

k. Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.
l. Passwords/passphrases must meet the following:
    i. Require a minimum length of at least eight characters.
    ii. Contain both numeric and alphabetic characters.
m. Change user passwords/passphrases at least once every 90 days.
n. Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
o. Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
p. Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.
q. Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.
r. Document and communicate authentication policies and procedures to all users including:
    i. Guidance on selecting strong authentication credentials
    ii. Guidance for how users should protect their authentication credentials
    iii. Instructions not to reuse previously used passwords
    iv. Instructions to change passwords if there is any suspicion the password could be compromised.
s. Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:
    i. Generic user IDs are disabled or removed.
    ii. Shared user IDs do not exist for system administration and other critical functions.
    iii. Shared and generic user IDs are not used to administer any system components.
t. Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.
u. Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:
    i. Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
    ii. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
v. All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

i. All user access to, user queries of, and user actions on databases are through programmatic methods.
ii. Only database administrators have the ability to directly access or query databases.
iii. Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

w. Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

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 8: USER ACCESS AND AUTHENTICATION POLICY

Approval guideline for IT use on the date specified.

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