DuPage County

Network Access and Authentication Policy	Created: 01/12/2016
Section of: County Security Policies	Modified:
Target Audience: Technical	Page 1 of 5

DuPage County is hereinafter referred to as "the County."

1.0 Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the County network are authenticated in an appropriate manner, in compliance with County standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

2.0 Scope

The scope of this policy includes all users who have access to County-owned or County-provided computers or require access to the County network and/or systems. This policy applies not only to County and County-wide Elected Official employees, but also to volunteers, contractors, and anyone requiring access to the County network. Public access to the County's externally-reachable systems, such as its County website or public web applications, are specifically excluded from this policy.

3.0 Policy

3.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.

- Users will be granted least amount of network access required to perform his or her job function.

- Users will be granted access only if he or she accepts the Technology Resources Acceptable Use Policy (Policy 8.1 in the DuPage County Employee Policy Manual).

- Access to the network will be granted in accordance with the Technology Resources Acceptable Use Policy (Policy 8.1 in the DuPage County Employee Policy Manual).

3.2 Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (Department Code + first, middle and last initials)

- Accounts must be password protected (refer to the Password Policy for more detailed information).

- Accounts must be for individuals only. Account sharing and group accounts are not permitted.

- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

- Occasionally guests will have a legitimate business need for access to the County network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the CIO or their designee or executive team, or as required by applicable regulations or third-party agreements.

3.3 Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the County, that employee's account can be disabled. Human Resources must notify the CIO or their designee in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.). Additionally, when an employee leaves employment at the County, the employee's supervisor must complete an "Information Technology Employee Separation Request" form, located on the intranet and submit this form to Information Technology. This form is to be completed at least 2 business days prior to the planned departure of an employee and as soon as possible, but not less than 7 days after an unplanned departure.

3.4 Authentication

User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

3.5 Use of Passwords

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the County's Password Policy.

3.6 Remote Network Access

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the County encourages additional scrutiny of users remotely accessing the network. The County's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.

3.7 Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are required to be activated after 15 minutes of inactivity.

3.8 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, antivirus software must be updated, as well as other critical software, to the latest versions before accessing the network. County IT may require that additional anti-malware and/or other security software be installed on computers that access the County network. This software will be provided by the County with instructions as to the installation.

3.9 Encryption

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the County network or across a public network such as the Internet.

3.10 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. The County will use software to lock accounts after ten (10) failed logons.

3.11 Non-Business Hours

While some security can be gained by removing account access capabilities during non-business hours, the County does not mandate time-of-day lockouts, however, in some instances deemed necessary by the Information Technology, time-of-day lockouts may be used.

3.12 Applicability of Other Policies

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

4.0 Definitions

Antivirus Software An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Biometrics The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Password A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Smart Card A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

Token A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

5.0 Revision History

Revision 1.0