DuPage County

Network Security Policy	Created: 01/12/2016
Section of: County Security Policies	Modified:
Target Audience: Technical	Page 1 of 13

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

1.0 Purpose

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the County's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

2.0 Scope

This policy covers all IT systems and devices that comprise the County network or that are otherwise controlled by the County. This policy also cover systems administered by County-wide Elected Officials.

3.0 Policy

3.1 Network Device Passwords

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords.

3.1.1 Password Construction

The following statements apply to the construction of passwords for network devices:

- Passwords must be at least 12 characters
- Passwords must be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords must not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords must not be comprised of an obvious keyboard sequence (i.e., qwerty)

- Passwords must not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

3.1.2 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. When possible, the County will lock accounts after five (5) failed logons.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

3.1.3 Change Requirements

Passwords must be changed according to the County's Password Policy. Additionally, the following requirements apply to changing network device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.

- If a County network or system administrator leaves the County, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.

- Vendor default passwords must be changed when new devices are put into service.

3.1.4 Password Policy Enforcement

Where passwords are used an application must be implemented that enforces the County's password policies on construction, changes, re-use, lockout, etc.

3.1.5 Administrative Password Guidelines

As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

3.2 Logging

The logging of certain events is an important component of good network management practices.

Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail the County's requirements for logging and log review.

3.2.1 Application Servers

Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers

Requirement: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

3.2.2 Network Devices

Logs from network devices are of interest since these devices control all network traffic, and can have a huge impact on the County's security.

Examples: Firewalls, network switches, routers

Requirement: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

3.2.3 Critical Devices

Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any cases where this occurs, this section shall supersede.

Examples: File servers, lab machines, systems storing intellectual property

Requirements: At a minimum, logging of errors, faults, and login failures is required. Additional logging is encouraged as deemed necessary. No passwords should be contained in logs.

3.2.4 Log Management

While logging is important to the County's network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, the County recommends that a log management

application be considered.

3.2.5 Log Review

Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events, however, a member of the County's IT team, or the Countywide Elected Officials IT Team, depending on the responsibility of said system, should still review the logs as frequently as is reasonable.

3.2.6 Log Retention

Logs will be retained for a minimum of 30 days. Unless otherwise determined by the CIO or their designee, logs should be considered operational data.

3.3 Firewalls

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the County network through the use of a firewall.

3.3.1 Configuration

The following statements apply to the County's implementation of firewall technology:

- Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

- No unnecessary services or applications should be enabled on firewalls. The County uses 'hardened' systems for firewall platforms, or appliances.

- Clocks on firewalls must be synchronized with the County's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

- The firewall ruleset must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.

- For its own protection, the firewall ruleset must include a "stealth rule," which forbids connections to the firewall itself.

- The firewall must log dropped or rejected packets.

3.3.2 Outbound Traffic Filtering

Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised. This will also prevent remote desktops from accessing the internal network.

The County encourages outbound filtering if possible, but it is not required. If filtering is deemed possible, only the following known "good" services should be permitted outbound from the network: 21, 22, 23, 25, 53, 80, 110, 443, and 995.

3.4 Networking Hardware

Networking hardware, such as routers, switches, hubs, bridges, and access points, should be implemented in a consistent manner. The following statements apply to the County's implementation of networking hardware:

- Networking hardware must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

- Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

- If possible for the application, switches are preferred over hubs. When using switches the County should use VLANs to separate networks if it is reasonable and possible to do so.

- Access control lists should be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.

- Unused services and ports should be disabled on networking hardware.

- Access to administrative ports on networking hardware should be restricted to known management hosts and otherwise blocked with a firewall or access control list.

3.5 Network Servers

Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to the County's use of network servers:

- Unnecessary files, services, and ports should be removed or blocked. Follow best practices for hardening Windows OS for Windows servers.

- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.

- A standard installation process should be developed for the County's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

- Clocks on network servers should be synchronized with the County's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

3.6 Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The County requires the use of both an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) on critical or high-risk network segments. Procedures must be implemented to review and act on the alerts expediently. For the IPS, procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic. The IPS must be audited and documented according to the standards detailed in the "Firewalls" section of this document.

3.7 Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the County's network security. Security testing can be

provided by IT Staff members, but is often more effective when performed by a third party with no connection to the County's day-to-day Information Technology activities. The following sections detail the County's requirements for security testing.

3.7.1 Internal Security Testing

Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the County's IT team. Internal testing does not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the CIO or their designee. Internal testing should have no measurable negative impact on the County's systems or network performance.

3.7.2 External Security Testing

External security testing, which is testing by a third party entity, is an excellent way to audit the County's security controls. The CIO or their designee must determine to what extent this testing should be performed, and what systems/applications it should cover.

External testing must not negatively affect network performance during business hours or network security at any time.

As a rule, "penetration testing," which is the active exploitation of County vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact County systems or data.

The County requires that external security testing be performed annually.

3.8 Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the County's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the County must be removed before disposal.

- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.

• Data wiping technology, which meets or exceeds Department of Defense standards, must be used on any hard drives prior to disposal. Simply reformatting a drive or erasing data does not make the data unrecoverable. If the data wiping technology is not possible, the device's data storage mechanism (such as its hard drive or solid state memory) must be destroyed.

3.9 Network Compartmentalization

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, the County will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The County requires the following with regard to network compartmentalization:

3.9.1 Higher Risk Networks

Examples: Guest network, wireless network

Requirements: Segmentation of higher risk networks from the County's internal network is required, and must be enforced with a firewall or router that provides access controls.

3.9.2 Externally-Accessible Systems

Examples: Email servers, web servers

Requirements: Segmentation of externally-accessible systems from the County's internal network is required, and must be enforced with a firewall or router that provides access controls.

3.9.3 Internal Networks

Examples: Finance, Human Resources

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. The County encourages, but does not require, such segmentation.

3.10 Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the County's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

At a minimum, network documentation must include:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses
- Access Control Lists

The County requires that network documentation be performed and updated on a yearly basis.

3.11 Minimum Configuration for Access

Any system, including but not limited to, workstations, tablets, notebooks, and servers, 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.

3.12 Software Use Policy

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The County provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for the County's software must be stored in a secure location.
- Open source and/or public domain software can only be used with the permission of the CIO or their designee.
- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.

- Vulnerability alerts should be monitored for all software products that the County uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

3.13 Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT Staff must perform the tasks before and after normal business hours. Tasks that are deemed "emergency support," as determined by the CIO or their designee, can be performed at any time.

3.14 Change Management

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT Staff should make a reasonable effort to document hardware and/or configuration changes to network devices in a "change log." If possible, network devices should bear a sticker or tag indicating essential information, such as the device name, IP address, Mac address, asset information, and any additional data that may be helpful, such as information about cabling.

3.15 Suspected Security Incidents

When a security incident is suspected that may impact a network device, the IT Staff should refer to the County's Incident Response policy for guidance.

3.16 Redundancy

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. The County wishes to provide the CIO with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability
- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite

3.17 Manufacturer Support Contracts

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the County must purchase a maintenance plan, support agreement, or software subscription that will allow the County to receive updates to the software and/or firmware for a specified period of time. The plan must meet the following minimum requirements:

Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time period, as determined by the CIO or their designee, as well as firmware or embedded software updates.

Software: The arrangement must allow for updates, upgrades, and hotfixes for a specified period of time.

3.18 Security Policy Compliance

It is the County's intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind the County requires the following:

3.18.1 Security Program Manager

An employee must be designated as a manager for the County's security program. He or she will be responsible for the County's compliance with this security policy and any applicable security regulations. This employee must be responsible for A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on the County's information security program (as detailed below), D) any ongoing testing or analysis of the County's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

3.18.2 Security Training

A training program must be implemented that will detail the County's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually.

3.18.3 Security Policy Review

The County's security policies must be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to the County's security policies. As part of this evaluation the County must review:

- Any applicable regulations for changes that would affect the County's compliance or the effectiveness of any deployed security controls.

- If the County's deployed security controls are still capable of performing their intended functions.

- If technology or other changes may have an effect on the County's security strategy.

- If any changes need to be made to accommodate future IT security needs.

3.19 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

ACL A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

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.

Firewall A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Hub A network device that is used to connect multiple devices together on a network.

IDS Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.

IPS Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

NTP Stands for Network Time Protocol. A protocol used to synchronize the clocks on

networked devices.

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

RAID Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.

Switch A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.

VLAN Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.

Virus Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

5.0 Revision History

Revision 1.0