Stark County Board of Developmental Disabilities

Policy 6.11 Network Security	Effective: 3/23/21
Chapter 6: Information Technology	Page 1 of 12

NETWORK SECURITY

POLICY

The Board wishes to provide a secure network infrastructure in order to protect the integrity of Board data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

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 Board'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.

This policy covers all IT systems and devices that comprise the Board network or that are otherwise controlled by the Board.

Historical Resolution Information		**Reviewer(s):**
Date	**Resolution Number**	Information Technology Manager
9/27/14	09-59-14	
1/30/18	01-12-18	
3/23/21	03-14-21	

NETWORK SECURITY

PROCEDURE

I. 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, servers, and security appliances, must be held to higher standards than standard user-level or desktop system passwords.

A. Password Construction

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

1. Passwords should be at least 8 characters
2. Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
3. Passwords should be comprised of a mix of upper and lower case characters
4. Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
5. Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
6. Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

B. Failed Logons

Repeated logon failures can indicate an attempt to “crack” a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the Board must lock a user's account after 5 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

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."

C. Change Requirements

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

1. If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
2. If a Board network or system administrator leaves the Board, 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.

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

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

E. 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.

II. 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 Board's requirements for logging and log review.

A. 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: Logging must be enabled to the fullest degree possible. No passwords should be contained in logs.

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

Examples: Firewalls, network switches, routers, security appliances

Requirement: Logging must be enabled to the fullest degree possible. No passwords should be contained in logs.

C. 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 and systems storing medical information

Requirements: Logging must be enabled to the fullest degree possible. No passwords should be contained in logs.

D. Log Management
While logging is important to the Board'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 Board recommends that a log management application be considered.

E. 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 Board's IT team should still review the logs as frequently as is reasonable.

F. Log Retention
Logs should be retained in accordance with the Board's Retention Policy. Unless otherwise determined by the IT manager, logs should be considered operational data.

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

A. Configuration
The following statements apply to the Board's implementation of firewall technology:

1. 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.
2. No unnecessary services or applications should be enabled on firewalls. The Board should use 'hardened' systems for firewall platforms, or appliances.
3. Clocks on firewalls should be synchronized with the Board's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
4. 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.
5. For its own protection, the firewall ruleset must include a "stealth rule", which forbids connections to the firewall itself.
6. The firewall must log dropped or rejected packets.

B. 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.

The Board requires that permitted outbound traffic be limited to only known "good" services, which are the following ports: 21, 22, 23, 25, 53, 80, 110, 443, and 995. All other outbound traffic must be blocked at the firewall unless an exception is granted from the IT Manager.

IV. 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 Board's implementation of networking hardware:

A. 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.

B. 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.

C. Only switches will be used for Board networking. No hubs will be allowed. When using switches the Board should use VLANs to separate networks if it is reasonable and possible to do so.

D. Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to the core switches should be limited to the greatest extent possible. Exceptions to this are management connections that can be limited to known sources.

E. Unused services and ports must be disabled on networking hardware.

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

V. 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 Board's use of network servers:

A. Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

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

C. If possible, a standard installation process should be developed for the Board's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

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

VI. 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 Board recommends the use of either an IDS or IPS on critical or high-risk network segments. If an IDS is used, procedures must be implemented to review and act on the alerts expediently. If an IPS is used, procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic. Also, if an IPS is used, it should be audited and documented according to the standards detailed in the "Firewalls" section of this document.

VII. Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the Board'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 Board's day-to-day Information Technology activities. The following sections detail the Board's requirements for security testing.

A. Internal Security Testing

Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the Board's IT team. Internal testing should 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 IT Manager. Internal testing should have no measurable negative impact on the Board's systems or network performance.

B. External Security Testing

External security testing, which is testing by a third party entity, is an excellent way to audit the Board's security controls. The IT Manager 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 Board vulnerabilities, should be discouraged. If penetration testing is performed, it must not negatively impact Board systems or data.

The Board encourages external security testing, but does not provide rigid guidelines regarding at what intervals the testing should occur. Testing should be performed as often as is necessary, as determined by the IT Manager.

VIII. Disposal of Information Technology Assets

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

A. Any asset tags or stickers that identify the Board must be removed before disposal.

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

C. At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, the Board must use the most secure commercially-available methods for data wiping. Alternatively, the Board has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid state memory).

IX. Network Compartmentalization

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, the Board 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 Board requires the following with regard to network compartmentalization:

A. Higher Risk Networks
Examples: Guest network, wireless network

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

B. Externally-Accessible Systems
Examples: Email servers, web servers

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

C. 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 Board encourages, but does not require, such segmentation.

X. 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 Board'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:

A. Network diagram(s)

B. System configurations

C. Firewall ruleset

D. IP Addresses

E. Access Control Lists

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

XI. Antivirus/Anti-Malware

Computer viruses and malware are pressing concerns in today's threat landscape. If a

machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire Board. The Board provides the following guidelines on the use of antivirus/anti-malware software:

A. All Board-provided user workstations must have antivirus/anti-malware software installed.

B. Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.

C. Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually

D. In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.

XII. 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 Board provides the following requirements for the use of software applications:

A. Only legally licensed software may be used. Licenses for the Board's software must be stored in a secure location.

B. Open source and/or public domain software can only be used with the permission of the IT Manager.

C. Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.

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

XIII. 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 IT Manager, can be performed at any time.

XIV. 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.

XV. Suspected Security Incidents

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

XVI. 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 Board wishes to provide the IT Manager 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:

A. Hard drive redundancy, such as mirroring or RAID

B. Server level redundancy, such as virtualization, clustering or high availability

C. Component level redundancy, such as redundant power supplies or redundant NICs

D. Keeping hot or cold spares onsite

XVII. Manufacturer Support Contracts

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the Board must purchase a maintenance plan, support agreement, or software subscription that will allow the Board 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 IT Manager, as well as firmware or embedded software updates.

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

XVIII. Security Policy Compliance

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

A. Security Program Manager

An employee must be designated as a manager for the Board's security program. He or she will be responsible for the Board's compliance with this security policy and any applicable security regulations. This employee must be responsible for:

1. The initial implementation of the security policies
2. Ensuring that the policies are disseminated to employees
3. Training and retraining of employees on the Board's information security program (as detailed in B. Security Training)
4. Any ongoing testing or analysis of the Board's security in compliance with this policy
5. Updating the policy as needed to adhere with applicable regulations and the changing information security landscape

B. Security Training

A training program must be implemented that will detail the Board'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. Additionally, the policies should be reviewed when there is an information security incident or a material change to the Board's security policies.

C. Security Policy Review

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

1. Any applicable regulations for changes that would affect the Board's compliance or the effectiveness of any deployed security controls
2. If the Board's deployed security controls are still capable of performing their intended functions
3. If technology or other changes may have an effect on the Board's security strategy
4. If any changes need to be made to accommodate future IT security needs

XIX. Applicability of Other Policies

This document is part of the Board'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.

XX. Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or

more severe penalties up to and including termination of employment. Where illegal activities or theft of Board property (physical or intellectual) are suspected, the Board may report such activities to the applicable authorities.

XXI. 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 Independent 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.