

Effective Date: 6/28/2005
Revised Date: 9/11/2017
Review Date: 9/11/2017

North Sound Behavioral Health Organization

Section 4000 – Information Systems: Server Security

Authorizing Source: North Sound BHO

Cancels:

See Also:

Responsible Staff: IS Specialist

Approved by: Executive Director

Signature:

Date: 10/3/2017

POLICY #4011.00

SUBJECT: SERVER SECURITY

PURPOSE

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by North Sound Behavioral Health Organization (North Sound BHO). Effective implementation of this policy will minimize unauthorized access to North Sound BHO proprietary information and technology.

SCOPE

This policy applies to server equipment owned and/or operated by North Sound BHO. This policy is specifically for equipment on the internal North Sound BHO network.

POLICY

A. Ownership and Responsibilities

All internal servers deployed at North Sound BHO shall be owned or leased by North Sound BHO. The Information System/Information Technology (IS/IT) Department is responsible for system administration.

Configuration changes for production servers must follow the appropriate change management procedures.

B. General Configuration Guidelines

1. Operating System configuration should be in accordance with specifications for the server task(s).
2. Services and applications that will not be used must be disabled where practical.
3. Access to services should be logged and/or protected through access-control methods.
4. The most recent security patches must be installed on the system as soon as practical; the only exception being when immediate application would interfere with business requirements.
5. Trust relationships between systems are a security risk and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

6. Always use standard security principles of least privilege to perform a function.
7. Do not use root/admin when a non-privileged account will do.
8. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSL/TLS or IPsec).
9. Servers will be physically located in an access-controlled environment and only authorized staff shall have physical access to them.
10. Servers are specifically prohibited from operating from uncontrolled office areas.

C. Monitoring & Log Retention

1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
 - a. All security related event logs will be exported four times a day.
 - b. Exported event logs will be zipped and saved in the following manner:
 - i. Folder name=property tag of server
 - ii. Four-digit year
 - iii. Two-digit month (e.g., 01. January)

yyyyymmdd-HHMM.zip where yyyyymmdd-HHMM is the date and time of the export.
 - c. Multiple copies of zipped event logs will be backed-up for both on and off-site storage.
 - d. Logs will be retained according to North Sound BHO retention policies.
2. Security related events will be monitored by the Security Officer, who will review logs and report incidents to the Privacy Officer. Corrective measures will be prescribed as needed. Security related events include, but are not limited to:
 - a. Port-scan attacks;
 - b. Evidence of unauthorized access to privileged accounts; and
 - c. Anomalous occurrences that are not related to specific applications on the host.
3. Security related events, like those listed above, do not necessarily indicate a security related incident.

D. Compliance

1. Audits will be performed on a regular basis by the Security Officer.
2. Security Officer will present audit findings and remediation recommendations to North Sound BHO Management Team.
3. Every effort will be made to prevent audits from causing operational failures or disruptions.

E. Enforcement

All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with North Sound BHO's Employee Conduct and Discipline Policy 3502.00.

ATTACHMENTS

None