Effective Date: 7/1/2019
Review Date: 5/24/2022
Revised Date: 4/26/2022

# North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Server Security

Authorizing Source: HCA Contract
Approved by: Executive Director Date: 5/24/2022 Signature:

**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 Administrative Services Organization (North Sound BH-ASO). Effective implementation of this policy will minimize unauthorized access to North Sound BH-ASO proprietary information and technology.

## SCOPE

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

## POLICY

1. **Ownership and Responsibilities**

   All internal servers deployed at North Sound BH-ASO shall be owned or leased by North Sound BH-ASO. The IT Department is responsible for system administration.

   Configuration changes for production servers must follow the appropriate change management procedures. See the IT Change management Policy and Procedures.

2. **General Configuration Guidelines**

   a. Operating System configuration should be hardened in accordance with specifications for the server task(s).
   b. Services and applications that will not be used must be disabled where practical.
   c. Access to services should be logged and/or protected through access-control methods.
   d. The most recent security patches on internal only servers must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements. Critical security patches must be installed on public facing Servers during the next patch window, preferably the day it is released. When that is not possible, critical patches will be installed within 72 hours of release.
   e. 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.
   f. Always use standard security principles of least privilege access to perform a function.
   g. Do not use root when a non-privileged account will do.
   h. 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 IPSec).
   i. Servers will be physically located in an access-controlled environment and only authorized staff shall have physical access to them.
   j. Servers are specifically prohibited from operating from uncontrolled office areas.

3. **Monitoring**
    a. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
        i. All security related event logs will be automatically forwarded to a logging server for auditing and archival purposes, or manually archived at a predetermined interval.
        ii. Exported event logs will be zipped and saved in the following manner:
            a) Folder name = property tag of server
                1) Four-digit year
                2) Month (e.g., 01. January)
                    i. yyyymmdd-HHMM.zip where yyyymmdd-HHMM is the date and time of the export.
        iii. Multiple copies of zipped event logs will be backed-up for both on and off-site storage.
        iv. Logs will be retained according to North Sound BH-ASO retention policies.
    b. Security-related events will be monitored by IT, who will review logs and report incidents to the Security Officer. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
        i. Port-scan attacks
        ii. Evidence of unauthorized access to privileged accounts
        iii. Anomalous occurrences that are not related to specific applications on the host.
    c. Security-related events, like those listed above, do not necessarily indicate a security-related incident.
4. **Compliance**
    a. Audits will be performed on a regular basis by the Security Officer.
    b. Security Officer will present audit findings and remediation recommendations to North Sound BH-ASO Leadership Team as needed.
    c. Every effort will be made to prevent audits from causing operational failures or disruptions.
5. **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 BH-ASO's Employee Conduct and Discipline policy.

**ATTACHMENTS**
None