| **POLICY & PROCEDURE**<br>**Configuration & Change Management** | | **POLICY #25** |
|---|---|---|
| **SUPERCEDES POLICY:** | **EFFECTIVE:** | **LAST REVIEWED:** |
| Privacy and Security Compliance Program<br>Exhibit L.B., Change Management | 3/1/2014 | **5/10/2024** |

## Purpose

To establish standards and controls for base configuration of servers and routers connected to Watershed Health, Inc. (Watershed) network or used in a production capacity.

## Applicability

All Watershed Workforce members are responsible for awareness of this policy and adherence to the given direction and guidance.

## Definitions

For definitions of capitalized terms or phrases, please refer to *Privacy, Security and Breach Notification Glossary.*

## Policy

Watershed will implement appropriate administrative, physical, and technical controls where appropriate and document and maintain configuration and change management processes for servers and routers. Results of the annual Risk Assessment that identify risks related to the change management process shall be considered, and changes to this Policy shall be included as needed.

## Procedures

1. In general, the Configuration and Change Management Program will
   a. Effectively manage and track configuration and associated document changes, as well as the integrity, availability and maintainability of the systems; and
   b. Ensure documented approval by Product Owner, CEO, or COO of changes to system components prior to production.
2. **Roles and Responsibilities.**
   a. Chief Technology Officer (CTO) or designee is responsible for:
      i. Approving and issuing policies, procedures, and guidance for implementing and coordinating the Watershed Configuration and Change Management Program;
      ii. Implementing the Configuration and Change Management Program, as appropriate;

   iii. Directing, monitoring, and enforcing implementation and maintenance of, and compliance with, the Configuration and Change Management Program; and

   iv. Overseeing periodic testing and evaluation of IT components to determine effectiveness and compliance with the Configuration and Change Management Program.

b. Server Administrators are responsible for:

   i. Installing and configuring systems in compliance with the organizational security policies and standard system and network configurations;

   ii. Maintaining systems in a secure manner, including frequent backups and timely application of patches;

   iii. Monitoring system integrity, protection levels, and security-related events:

      (1) Ensure necessary settings are configured on the host to allow collection of qualified events into the SIEM;

      (2) Security-related events include, but are not limited to:

         (a) Port-scan attacks;

         (b) Evidence of unauthorized access to privileged accounts;

         (c) Anomalous occurrences that are not related to specific applications on the host; and

         (d) Host compromise or infection.

   iv. Following up on detected security anomalies associated with their information system resources; and

   v. Conducting security tests as required.

c. Product Owner, CEO, or COO is responsible for:

   i. Documenting approval of changes to system components prior to production.

d. Cybersecurity Oversight Committee is responsible for:

   i. Monthly review of changes to system components; and

   ii. Monthly review of documented approval of changes by Product Owner, CEO, or COO prior to production.

e. Security Officer, or designee, is responsible for:

   i. Weekly review of vulnerability reports;

   ii. Presenting monthly report of identified vulnerabilities, criticality determinations, and recommended remediations to Cybersecurity Oversight Committee;

   iii. Determining criticality of vulnerabilities (if any);

   iv. Immediately remediating critical patches; and

v. Putting non-critical patches into regular change cycle.

3. **Server Configuration and Management.**

a. Secure server software installation.

i. Install only approved operating systems from an approved source, the services required for the server, and to eliminate any known vulnerabilities through patches or upgrades.

ii. Any unnecessary applications, services, or scripts that are installed should be removed immediately once the installation process is complete.

iii. During the installation of the server software, the following steps should be performed:

(1) Install the server software either on a dedicated host or on a dedicated guest OS if virtualization is being employed

(2) Apply any patches or upgrades, as soon as practicable, to correct for known vulnerabilities in the server software

(3) Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable

(4) Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration)

(5) Remove or disable all unneeded default user accounts created by the server installation

(6) Remove all manufacturers' documentation from the server.

(7) Remove all example or test files from the server, including sample content, scripts, and executable code.

(8) Remove all unneeded compilers.

(9) Apply the appropriate security template or hardening script to the server.

(10) For external-facing servers, reconfigure service banners not to report the server and OS type and version, if possible.

(11) Configure warning banners for all services that support such banners.

(12) Configure each network service to listen for client connections on only the necessary TCP and UDP ports, if possible.

b. Configure access controls.

i. Server administrators should consider how best to configure access controls, in accordance with *Security Policy #14, Access Control*, to protect information stored on servers from two perspectives:

(1) Limit the access of the server application to a subset of computational resources.

(2) Limit the access of users to the security principles of least privilege and through any additional access controls enforced by the server, where more detailed levels of access control are required.

ii. Access controls can enforce separation of duty by ensuring server logs cannot be modified by server administrators and potentially ensure that the server process is only allowed to append to the log files.

(1) Typical files to which access should be controlled are:

(a) Application software and configuration files;

(b) Files related directly to security mechanisms:

(i) Password hash files and other files used in authentication;

(ii) Files containing authorization information used in controlling access; and

(iii) Cryptographic key material used in confidentiality, integrity, and non-repudiation services;

(c) Server log and system audit files;

(d) System software and configuration files; and

(e) Server content files.

c. Authentication and encryption technologies.

i. Systems storing sensitive or confidential information should implement cryptographic protection of this data.

ii. Business units should work with System Administrators to ensure encryption meets cryptographic use and business requirements.

d. Physical access controls (as applicable).

i. Servers should be physically located in an access-controlled environment, in accordance with *Security Policy #10, Facility Access Controls*.

ii. Servers operating from uncontrolled areas are prohibited.

iii. Servers whose functionality is critical to core business functions and have been deemed critical should have a Disaster Recovery Plan, dependent on Watershed's control on the environment, in accordance with *Security Policy #7, Contingency Plan*, that includes data replication and backup and recovery procedures.

4. **Router Configuration and Management.**

a. Watershed is a remote workforce and is no longer relying on a physical work environment and router functionality.

## Enforcement

Violations of this policy will result in imposition of sanctions in accordance with Watershed sanctions policy. This may include suspension or loss of the violator's use privileges, with respect to Watershed's information systems, termination of employment or volunteer, intern, contractor status with Watershed. Additional civil, criminal and equitable remedies may apply.

## Documentation

The CTO or designee is responsible for ensuring this version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, will be retained by Watershed for a period of at least 6 years plus the current year from the date of creation or the date when last in effect, whichever is later.

## References

### Regulatory Authority:

1. 45 C.F.R. §164.308 (a) (7)(i) – Standard: Contingency Plan.
2. 45 C.F.R. §164.308 (a) (7)(ii) – Implementation specifications.
3. 45 C.F.R. §164.310(a)(1) – Standard: Facility access controls.
4. 45 C.F.R. §164.310(a)(2)(i) – Contingency operations (Addressable).
5. 45 C.F.R. §164.310(a)(2)(ii) – Facility security plan (Addressable).
6. 45 C.F.R. §164.310(a)(2)(iii) – Access control and validation procedures (Addressable).
7. 45 C.F.R. §164.312(a)(1) – Standard: Access control.
8. 45 C.F.R. §164.312(a)(2) – Implementation specifications.

### Internal:

1. Security Policy #7, Contingency Plan
2. Security Policy #10, Facility Access Controls
3. Security Policy #14, Access Controls

### External:

1. Current Administrative Simplification Regulations
2. Refer to *NIST Publications Reference Guide* for specific guidance

## Document Control

| APPROVED BY: | | |
|---|---|---|
| **Lisa Stanley** | 5/28/2024 | DocuSigned by:<br>Lisa Stanley<br>9418DCC7CF3D47D... |
| **(Printed Name)** | **(Date)** | **(Signature)** |

| REVISION HISTORY | | | |
|---|---|---|---|
| **Date** | **Author** | **Version** | **Comments** |
| 3/1/2014 | Arthur Grant | 1.0 | Implemented |
| 2/19/2015 | Lisa Stanley | 2.0 | Reviewed |
| 2/23/2016 | Lisa Stanley | 3.0 | Reviewed |
| 1/30/2017 | Lisa Stanley | 4.0 | Reviewed |
| 3/3/2018 | Lisa Stanley | 5.0 | Reviewed |
| 9/3/2019 | Lisa Stanley | 6.0 | Reviewed |
| 3/18/2020 | Lisa Stanley | 7.0 | Reviewed |
| 11/13/2020 | Scott Snodgrass | 8.0 | Reviewed and updated by Privacy & Security Officer |
| 11/11/2021 | Lisa Stanley | 8.0 | Reviewed |
| 5/20/2022 | Lisa Stanley | 8.0 | Reviewed |
| 5/17/2023 | Nicole Montagnet | 9.0 | Reviewed and updated by Privacy & Security Officer |
| 5/10/2024 | Nicole Montagnet | 9.0 | Reviewed |