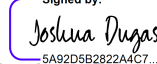




DBH-IT Maintenance Policy

Effective Date
Revised Date

08/26/2026
08/26/2026

Signed by:

SA92D5B2822A4C7...
Joshua Dugas, MBA, REHS, Director

Policy

It is the policy of the Department of Behavioral Health (DBH) Information Technology Department (DBH-IT) to establish and maintain a healthy infrastructure and system environment by ensuring security controls are in place to protect the routine maintenance activities that enable technology systems to function properly. This policy applies to all DBH systems and users of DBH information systems.

Purpose

To provide guidance to DBH IT to ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of DBH information system resources.

Definition(s)

Application Program: Software program that runs on your computer. Web browsers, e-mail programs, word processors, and utilities are all applications.

Information Systems: Interrelated components working together to collect, process, store, and disseminate information to support decision-making, coordination, control, analysis, and visualization in an organization.

Operating System (OS): Software that acts as an interface between computer hardware components and the user.

Routine Maintenance: Activities include diagnosing and correcting hardware, firmware, and software problems; loading, maintaining, and updating software, device drivers, configuration settings, etc., and maintaining a historical record of system changes.

Continued on next page

DBH-IT Maintenance Policy, Continued

Roles and Responsibilities

All personnel involved in the maintenance of information systems and supporting infrastructure are responsible for adhering to this policy and with any additional internal maintenance requirements:

Role	Responsibility
Business Application Manager	• Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, and • Explicitly approve the removal of information system or system components from organizational facilities for off-site maintenance or repairs.
Department Systems Analyst	• Control and monitor the use of information system maintenance tools; • Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; • Check all diagnostic and test program media for malicious codes prior to use; • Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions. Whenever possible, utilize two-factor authentication on remote maintenance ports; • Following maintenance or repair actions check all potentially impacted security controls to verify the controls are still functioning properly, and • Ensure access to appropriate sanitizing equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs in accordance with the Data Sanitization Policy.

Continued on next page

DBH-IT Maintenance Policy, Continued

Roles and Responsibilities continued

Role	Responsibility
Department Systems Analyst (continued)	• Ensure remote maintenance port access is normally blocked unless unattended access is required. Whenever possible, require involvement of DBH-IT opening remote maintenance ports; • When maintenance is completed, terminate all sessions and remote connections; • Allow only authorized personnel to perform maintenance on DBH information systems; • Maintain a list of authorized maintenance personnel including third-party maintenance providers, and • Organizational personnel with appropriate access authorizations and sufficient technical competence shall supervise maintenance personnel during the performance of information system maintenance activities.
Third Parties	• Third party service providers with systems interconnected to the San Bernardino (SB) County network are responsible for maintaining their systems in accordance with this policy.

Operating System Maintenance

Support for Operating Systems:

DBH-IT shall ensure the operating systems used to run the production environment are regularly monitored for security risks and maintained in approved secure configurations to support DBH operations, including log review and daily maintenance tasks.

Operating System Software Upgrades:

- Operating system (OS) upgrades shall be carefully planned, executed and documented.
- System security controls shall be reviewed when upgrades occur and documentation will be updated as appropriate.
- DBH-IT shall review change control procedures to include:
 - Upgrade certification,
 - User acceptance testing, and
 - To establish a rollback plan to ensure compliance with state and federal regulations.

Continued on next page

DBH-IT Maintenance Policy, Continued

Maintenance Documentation

The following documentation requirements, based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations; shall be applied to information systems which if unavailable would cause a moderate to severe impact to organizational productivity or services.

Maintenance Records:

Maintain information system maintenance records for the life of the system that include:

- Date and time of maintenance;
- Name(s) of the individual(s) performing the maintenance;
- Name of escort (if necessary);
- Description of maintenance performed, and
- List of equipment removed or replaced (including identification numbers if applicable).

Third-Party Maintenance Personnel:

Third-party maintenance providers under contract to perform maintenance/support services on DBH information systems shall provide a list of field service engineers assigned to support DBH maintenance contract with the following information for each service representative:

- Name;
- Company represented;
- Title;
- Contact Info (phone number; e-mail);
- Photo for identification purposes, and
- List of systems on which individual is authorized to perform maintenance.

Notification of Downtime

Any planned system maintenance causing downtime to users shall require prior notification of no less than 24 hours to affected DBH workforce members and contract providers.

Related Policy or Procedure

DBH Standard Practice Manual and Forms:

- Device and Media Controls Policy (IT5008)
- Data Sanitation Policy (IT5016)

Reference(s)

- [National Institute of Standards and Technology \(NIST\) Publication 800-53](#)
-