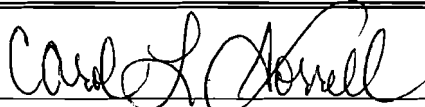
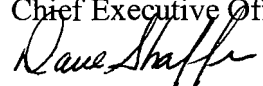
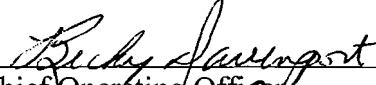

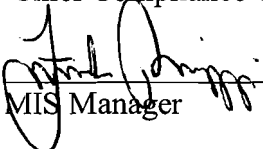


**KERN HEALTH SYSTEMS  
POLICIES AND PROCEDURES**

SUBJECT: Server Security		INDEX NUMBER 7.03		Page 1 of 3			
SECTION: MIS		ISSUE DATE <i>April 4, 2006</i>					
Review Date							
Effective Date							
Revision No.							

Approved		Date	<i>4/3/06</i>
	Carol Sorrell, R.N. Chief Executive Officer		
Approved		Date	<i>3-22-06</i>
	Chief Financial Officer		
Approved		Date	<i>3-29-06</i>
	Chief Operating Officer		
Approved		Date	<i>3-20-06</i>
	Chief Compliance Officer		
Approved		Date	<i>3-20-06</i>
	MIS Manager		

**POLICY<sup>1</sup>:**

This policy applies to server equipment owned and/or operated by Kern Health Systems (KHS), and to servers registered under any KHS owned internal network domain.

This policy is specifically for equipment on the internal KHS network. For secure configuration of equipment external to KHS on the DMZ, refer to the *Internet DMZ Equipment Policy*.

**PURPOSE:**

To establish standards for the base configuration of internal server equipment that is owned and/or operated by KHS. Effective implementation of this policy will minimize the risk of unauthorized access to KHS proprietary information and technology.

This policy is specifically for equipment on the internal KHS network. For secure configuration of equipment external to Kern Health Systems on the DMZ, refer to the *Internet DMZ Equipment Policy*.

**KERN HEALTH SYSTEMS  
POLICIES AND PROCEDURES**

SUBJECT: Server Security	INDEX NUMBER 7.03	Page 2 of 3
--------------------------	----------------------	-------------

**DEFINITIONS:**

DMZ	De-militarized Zone. A network segment external to the corporate production network
Server	For purposes of this policy, a Server is defined as an internal KHS Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

**PROCEDURE:**

**1.0 Responsibilities**

All internal servers deployed at KHS are the responsibility of the MIS Department.

- A. Server patches and security updates must be kept up-to-date.
- B. Configuration changes for production servers must follow the appropriate change management procedures.

**2.0 General Configuration Guidelines**

- ❖ Operating System configuration should be in accordance with MIS guidelines.
- ❖ Services and applications that will not be used must be disabled where practical.
- ❖ Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- ❖ 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.
- ❖ 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.
- ❖ Always use standard security principles of least required access to perform a function.
- ❖ Do not use root when a non-privileged account will do.
- ❖ 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 SSH or IPsec).
- ❖ Servers should be physically located in an access-controlled environment.
- ❖ Servers and security-related devices are specifically prohibited from operating from uncontrolled cubicle areas.

**3.0 Monitoring**

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows: all security related logs will be kept online for a minimum of one week, daily incremental tape backups will be retained for a least one month, weekly full tape backups of logs will be retained for at least one month, and monthly full backups will be retained for a minimum of two years.

---

**KERN HEALTH SYSTEMS  
POLICIES AND PROCEDURES**

SUBJECT: Server Security	INDEX NUMBER 7.03	Page 3 of 3
--------------------------	----------------------	-------------

Security-related events will be reported to MIS, who will review logs and report incidents to management. 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
- C. Anomalous occurrence that are not related to specific applications on the host

**4.0 Compliance**

Audits will be performed on a regular basis by MIS, audits will be managed by AIS Internal Auditor or MIS in accordance with the Audit Policy. MIS will filter findings not related to a specific operational group and then present the findings to the appropriated support staff for remediation or justification. (See Attachment A).

Every effort will be made to prevent audits from causing operational failures or disruptions.

**5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Attachments:**

- Attachment A: Server Audit Report

---

<sup>1</sup> Revision 2006-04:

