**POLICY**

Only the Division of Information Technology or its designees may authorize the connection of a server to the University network. Servers shall be authorized only for those activities that directly support the education, research, public service or health care missions of the University. Server ports shall be limited to only those necessary to accomplish the functions being served.

1. **Definitions:**

   Administrator: means any individual who operates or maintains a University server or network, including, if appropriate, data custodians.

   Authentication: means the process used to determine the identity of a user.

   Server: Computer that shares resources (applications, files, etc.) with other computers (ie, clients) on a network. Servers shall be given 'static' (persistent) IP addresses.

2. **Access Control:** Access to University servers and networks is tightly controlled to shield University systems from vulnerabilities. If an administrator is not a University employee (ie a consultant or student assistant), DoIT staff shall set up the access control systems including firewalls, reverse proxies and similar technologies.

   Servers shall be located in a secured space with access strictly limited to only those individuals authorized to administer or maintain them.

   Each administrator shall insure that:

   - only authorized users have access to the server;
   - passwords for servers that use only User ID / Password authentication are changed on a periodic basis;
   - administration of the server is local or through the use of an encrypted session;
   - server access is limited through the use of control systems such as host-based firewalls or similar technologies;
   - servers containing critical University records are backed-up on a routine basis to protect the integrity of data, with back-up media stored offsite.

   Each administrator shall insure that access to information stored on servers under their direct control complies with the requirements of FERPA, HIPAA, the Gramm-Leach-Bliley Act and other applicable laws. See DoIT 100.

3. **Connecting Servers to the University Network:** Before a new server may be connected to the University network, the following data shall be provided the University TeLNet Services for review:

   A. Owner of record (department or project name)
   B. Contact information for responsible person (name, pager, emergency phone)
   C. Name of the administrator (sysadmin)
   D. Server location, building and room
   E. Server make, model
   F. Server purpose
G. Operating System, vendor, version number and patches applied
H. MAC address
I. Requested server name
J. Status of patches necessary to eliminate known vulnerabilities If DoIT approves the application, TeLNet shall issue the server a static IP address.

No system will be connected to the campus network unless all vendor supplied passwords have been changed from their default values.

4. Server Maintenance:

A. Administrators shall maintain and upgrade the operating system and applications for each server under their jurisdiction.
B. Server software shall be upgraded when necessary.
C. Administrators shall monitor software vendor announcements and other resources to determine the need to apply patches to software, and shall apply patches to operating systems and applications as often as practical. Critical patches shall be applied immediately on availability.
D. Servers that contain vulnerabilities may be removed from the network until properly updated. DoIT may scan any server connected to the University network for known or suspected vulnerabilities at any time, without notice.
E. Disposal of Servers: Administrators shall remove all data, including all software from server hard disks before the server or its storage media is sent to Property Control, transferred to another unit, discarded or repurposed. Data removal must be done in such a manner that it cannot be recovered. If necessary, DoIT’s Client Support Office shall assist with purging a server of data and software.

INQUIRIES/REQUESTS:

Office of the Chief Information Officer
Room 231, Educational Communications Center