Policy Statement Concerning University Computer Servers

Computer servers (computers that provide services to more than one user) that contain private data must either be housed within the University's Data Center to benefit from the following list of safeguards or must provide the following list of safeguards if not housed within the University's Data Center.

Computer servers that contain private data:

- Must have adequate physical security.
- Must have adequate environmental protection.
- Must be kept up-to-date with vendor security patches.
- Must have current antivirus software and current definition files which must be kept up-to-date.
- Must have either a host-based firewall or network-based firewall protecting the system.
- Must have a strong administrator password that will not be shared with others.
- Must have strong passwords for all areas where private data is stored.
- Must have an identified owner/administrator who will be responsible for issues concerning the operation of the server.
- Must be "backed up" for business continuity.
- Must have a log identifying changes to the server.
- Must be in compliance with regulations concerning the privacy and safeguarding of private data.

Note: Private data is defined as any data that is not publicly available data. For example a phone number is publicly available, unless the owner opted to not make the data public. A social security number is considered private data.

(rev. 6-6-05)