POLICY TITLE	Responsibility for Security of Computing Devices Connected to the UVU Network	**Policy Number**	447
Section	Facilities, Operations, and Information Technology	**Approval Date**	October 14, 2004
Subsection	Information Technology	**Effective Date**	October 14, 2004
Responsible Office	Office of the Vice President of Information Technology		

1.0 PURPOSE

1.1 The purpose of this policy is to clearly define requirements for owners and overseers of UVU network-connected devices to close security gaps. It also describes loss of network access for noncompliance, as well as an exception process.

2.0 REFERENCES

3.0 DEFINITIONS

4.0 POLICY

4.1 Those responsible for devices connected to the UVU network must ensure that key security vulnerabilities are eliminated from these devices.

4.2 Although the rapid growth of legitimate new uses of the Internet is quite welcomed, this growth has at the same time increased the opportunities and temptations for misuse of the Internet resource. Security breaches at highly visible computing sites have become commonplace today, and universities are favorite targets for attacks. Critical university computing resources, such as research, patient care, and student data, are at risk, and university computing devices are being commandeered by cyber-criminals to launch attacks on corporations and other entities outside the University. While it is not possible to anticipate and intercept all attacks—cyber-criminals are continuously devising new ways to wreak havoc—there are specific steps that can be taken to significantly reduce vulnerability. These steps are effective, however, only if they are taken for all devices on the UVU network. The saying that "we are only as strong as our weakest link" most definitely applies in this case. Key security gaps that need to be closed may vary depending upon the type of device. It is important to note that the following examples do not represent a complete list of known security vulnerabilities.

4.2.1 All device owners shall ensure passwords used on their devices are not easily guessable by attackers.

4.2.2 Owners of personal computers shall install and run anti-virus software on these devices and apply updates from the software vendor as they become available.

4.2.3 Owners of personal computers and servers shall apply security-related updates to the operating system running on their devices as these updates become available from operating system vendors.

4.2.4 Owners of servers and personal computers shall switch off unneeded services and/or use a firewall to eliminate the risk of these being exploited.

4.2.5 Vulnerabilities that are considered "key" will change over time as new threats and risks surface. Office of Information Technology (OIT) maintains and communicates a current list of key vulnerabilities and steps required to close the vulnerabilities. Device owners are responsible for staying apprised of changes to this list and acting promptly to address any new security gaps defined. OIT shall work in partnership with owners and overseers in fulfilling the responsibilities outlined in this policy.

4.3 Scope

4.3.1 This policy applies to anyone in the University community owning or overseeing the use of any type of computing device connected to the UVU network, including but not limited to:

1) OIT, if the devices are under ongoing support contracts;

2) Faculty, staff, students, and other individuals who have devices connected to the UVU network, even if those devices were acquired personally, i.e., not with university or grant funds;

3) UVU department heads, even in cases where vendor-owned and/or vendor-managed equipment is housed in departments;

4) Project principal investigators, if their projects use devices connected to the UVU network.

4.3.2 If no one claims responsibility for a device, the UVU department head for the department in which the device resides shall be presumed to be responsible by default. This policy is especially focused on individuals responsible (as defined above) for devices that serve more than one user; however, the required actions outlined in this policy are appropriate and must be undertaken by those responsible for single-user devices as well. When devices are used for university business, compliance shall be verified by Internal Audit during routine audits.

4.4 Enforcement

4.4.1 In cases where university network resources and privileges are threatened by improperly maintained computing devices, OIT may act on behalf of the University to eliminate the threat by working with the relevant device owner to quickly close security holes. In circumstances where these collaborative efforts fail or there is an urgent situation requiring immediate action and leaving no time for collaboration, the device may be disconnected from the network by OIT.

4.5 Exceptions

4.5.1 Requests for exceptions to this policy shall be made in writing (hard copy or email) to the Chief Information Officer. Exception may be granted if it is clear that the benefits to the University far outweigh the risks of the vulnerable device, as judged by the Associate Vice President of Information Technology.

4.6 Review Frequency

4.6.1 Reviewed yearly by the Chief Information Officer.

5.0 PROCEDURES

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity