

# University of Kentucky

## Patch Management and Virus Protection Policy

09/19/2003

### Statement of Necessity

Due to the continually increasing dependence of University systems on the security and integrity of our computer network, servers, and workstations, it has become vitally important that the University be more proactive about identifying and enforcing security standards. In particular, university computers must be properly patched with the latest appropriate updates to reduce the vulnerability of the entire community to malicious attacks. University computers must also have proper virus protection software and current virus definition libraries. These policies apply to all servers and workstations on the University network or performing University functions.

### Responsibilities and Practices of the Unit

Each department of the University is responsible for the proper usage of their computing and network resources, as spelled out in the [UK Policy Governing Access and use of UK Computing Resources](#). Specifically: *User access to computing resources is contingent upon prudent and responsible use; Computing resources must be shared among users in an equitable manner; The user may not participate in any behavior that unreasonably interferes with the fair use of computing resources by another.*

Any individual assigned a computer (server or workstation) on the university network or accessing university resources using a non-university computer has the following responsibilities:

1. **Patch Management** – The computer must have a regular schedule or automated process for identifying and loading appropriate security updates for the operating system or other software. For Microsoft Windows this will often be use of the auto update feature with the Windows Update Web site (<http://windowsupdate.microsoft.com>).
2. **Virus Protection** – The computer must have the university virus protection software, or a comparable alternative, loaded on the machine. In addition, the virus definition libraries must be updated on a regular basis (generally checked at least once a week) preferably through the auto update feature of the software.

Any unit of the University which is running a networked server<sup>1</sup> has the following additional responsibilities:

1. **Domain Names** – The server(s) must be assigned a name on the university domain, uky.edu, regardless of where it is housed.
2. **Server Support** – The unit must provide dedicated technical staff to serve as server administrator(s) to conduct all standard and required maintenance on the server(s) or to coordinate with system vendors for that maintenance. The server administrator(s) must apply appropriate patches and updates in a timely manner to both the operating system and any and all other software which require patches or updates, or work with system vendors to ensure appropriate patches and updates are applied or incorporated; conduct log audits and system audits on a regular basis; disable any and all unneeded services, ports and programs on the server(s); load and maintain virus protection software; and carry out any other security measures deemed necessary.
3. **Server Installation** – Whenever and to the extent possible initial server setup should occur prior to connecting the server to the network. After a new server is set up, but before any new server is put into active service, the unit will conduct a security audit and evaluation in coordination with Information Technology to verify that the server meets security needs and obligations and that all software on the server is properly patched and updated.
4. **Notification to Information Technology** – The unit will notify Information Technology any time a new server is brought online indicating any special requirement(s) of those servers, primary and secondary contact information, and identification of IP addresses.<sup>2</sup>
5. **Coordination with Information Technology** – The unit server administrator(s) must subscribe to, monitor, and participate with appropriate e-mail lists of Information Technology for security and system availability. The unit server administrator(s) must notify Information Technology of all security breaches in the minimum time possible.<sup>3</sup>

---

<sup>1</sup> A server is a computer which distributes information across the network to a wide audience of other, client, machines. Web servers are the most visible type of server. However, many workstations may be operating as servers because approved testing, research or collaboration software has been installed, or as unapproved servers because file sharing software (e.g., KAZAA) has been installed. Any computer performing the functions of a server must meet the requirements of this policy even if it is also an individual's workstation.

<sup>2</sup> Notification should be accomplished via email to [incident@lsv.uky.edu](mailto:incident@lsv.uky.edu).

<sup>3</sup> Notification should be accomplished via email to [incident@lsv.uky.edu](mailto:incident@lsv.uky.edu).

## **Responsibilities and Practices of the Department of Information Technology**

1. **Network Scans** – Information Technology (IT) will conduct scans of the University network to identify known vulnerabilities. IT will maintain logs of these vulnerabilities to identify patterns of behavior of concern. IT will identify appropriate scans for any organizational subset of the campus requiring more specific scans. IT will provide server administrators with appropriate information to recognize such scans from IT in their logs. Only IT or units approved by IT may conduct such scans.
2. **Reporting** – When IT learns of a vulnerability or security breach, they will notify the responsible unit in the minimum time possible.
3. **Communication** – IT will maintain e-mail lists for communication of regular security and system issues. In cases of severe vulnerabilities IT will, at their discretion, work to communicate these hazards more broadly.

## **Vulnerability Response Process and Responsibilities**

1. If a unit or individual identifies a vulnerability on one of the unit's computers, the unit or individual will act to close that vulnerability in the minimum time possible. If this is believed to be an unidentified vulnerability, unit staff will notify Information Technology immediately.<sup>4</sup>
2. If IT, through its scans or other means, identifies a vulnerability on a unit's computer(s), IT staff will notify the unit of the problem in the minimum time possible and of an appropriate window within which to close the vulnerability. If no time is specified the unit has two weeks to close the vulnerability.
3. If after notifying the unit and any other subsequent actions deemed appropriate by IT, the vulnerability remains, IT staff will take all necessary actions, including disconnecting the computer from the network, to protect other computers and the integrity of the university computing environment.

---

<sup>4</sup> Notification should be accomplished via email to [incident@lsv.uky.edu](mailto:incident@lsv.uky.edu).

### **Special Requirement for Web Servers**

Because of the special vulnerability of Web servers and the ease and frequency with which they are set up on campus, server administrators need to be able to track down any server as a source of dangerous or malicious activity. To that end, IT will establish a Web site to track the name, IP and contact information for all Web servers on campus not directly supported by IT. Server administrators are required to maintain their Web server information on this Web site.