

# **Virus Response Plan**

This plan provides a framework to assess virus risks, communicate accurate virus information, contain virus outbreaks quickly, and prevent future infections.

## **Categories of Responses:**

- No alert: Virus is confirmed a hoax.
- Minimal alert: Rare or scattered reports. Data gathering and internal notification (IT Services) needed.
- Moderate alert: National news coverage, multiple KUSM-W reports, significant risks identified. Campus-wide notification needed.
- High alert: Many confirmed KUSM-W reports, suspension of normal services. Full incident handling or disaster recovery procedures required.

## **Preventive Measures:**

1. KU Medical Center has a site license for virus protection software.
2. Virus detection software is installed on all KUSM-W workstations.
3. Virus detection software is installed at the email gateway and on all file servers.
4. DAT files are updated on a weekly basis, or more frequently when necessary.
5. Alert is emailed to IT Services when virus is detected.
6. Antivirus software configuration is password-protected to prevent unauthorized changes.

## **Notification Procedures:**

1. Monitor alert services for announcements regarding virus threats – IT Services
2. Check hoax list at McAfee or Symantec before forwarding any virus announcement – everyone
3. Report virus infections to IT Services – everyone
4. Document reported infections – IT Services
5. Gather data, assess extent of damage (mapped drives), and recommend appropriate actions (DAT update, cleaning utility, etc.) – IT Services
6. Alert Assistant Director of IT Services and network specialists upon receiving multiple reports of a high-risk virus – IT Services
7. Program gateways to block the virus from entering the campus – network specialists, KUMC network development
8. Issue a campus broadcast message, including virus description, extent of outbreak, vulnerable computers, removal instructions and preventive measures – IT Services
9. Distribute updated DAT files – IT Services
10. Clean infected computers and restore damaged files from backups if necessary – IT Services

## **Contact information**

Contact IT Services with any questions or problems  
316-293-2605 or e-mail [techsupp@kumc.edu](mailto:techsupp@kumc.edu)