

# Virus Event Standard Operating Procedures

In the event of a virus attack or other malicious attack on City computing resources the following procedures will be used in responding to the event.

## 1. Event oversight

In most cases news of an attack will come from the help desk, news reports, or on-call personnel. Once we become aware of an event calls will be made to the following staff in sequential order. The first person contacted will be responsible for oversight:

Work

Home

Pager/Cell

## 2. Technical Supervision

The person contacted in step 1 above will place calls to the following supervisors in order until the first contact is made.

## 3. Technical Assistance – Servers and E-mail

The person contacted in step 2 above will place calls to the following technicians in order until the first contact is made.

### Technical Assistance - Workstations

The person contacted in step 2 above will place calls to the following technicians in order until the first contact is made.

## 4. Server/Exchange E-mail procedures

- 1.) Assess situation and determine risk factors
- 2.) Depending upon level of risk, any of the following steps may be taken:
  - Shut down individual mailboxes (those known to be infected)
  - Stop mail service – externally and internally
  - Acquire, test, install new virus pattern files
  - Manual scan of servers and mail store
    - Delete attachments
    - Quarantine attachments
    - Strip specific file types
  - Shut down servers
  - Assess and repair damage

## 5. Workstation Procedures

- 1.) Assess situation and determine risk factors
- 2.) Depending upon level of risk, any of the following steps may be taken:
  - Shut down infected workstations
  - Remove infected workstations from network
  - Acquire, test, install new virus pattern files
  - Modify scanning frequency
  - Assess and repair damage

## 6. Communications

- 1.) Notify and inform Help Desk Supervisor
- 2.) If necessary, notify City staff

- Voicemail announcement
- Department contacts
- Special meeting
- E-mail
- Intranet
- Signs/fliers

3.) If necessary, convene EOC