

Polk County Government
ADMINISTRATIVE SAFEGUARDS
Information Access Management
Protecting Polk County Information Systems Policy and
Procedures

Policy 603.F

Effective: March 15, 2005

Revision Date:

I. Policy

- A. Polk County Government will develop, implement and monitor protection from malicious software, viruses, and breach of security including procedures for guarding against, detecting and reporting malicious software, viruses, and breach of security.
- B. The Information Technology Department will be responsible for development, implementation and monitoring of procedures that will provide protection from malicious software, viruses, and breach of security including procedures for guarding against, detecting and reporting malicious software, viruses, and breach of security.
- C. The Information Technology Department, in coordination with Department Heads or Division Supervisors will implement, as an integral component of Polk County Government's Security Awareness and Training, security reminders that provide periodic reminders relating to security updates and safeguards.

II. Procedures

- A. The Information Technology Department will be responsible for development, implementation and management of processes for guarding against, detecting and reporting malicious software, viruses, and breach of security.
- B. Protections to be implemented may include:
 - 1. Virus protection software. This procedure should include initial installation and requirements for updating the software. All computers and servers in Polk County's information system shall have virus protection software installed.
 - 2. Testing for viruses. This procedure should require scheduled testing of optical, digital, and magnetic media for viruses or malicious programs or program scripts before loading onto any workstation or server.

3. Third party software. This procedure should address the use and installation of Intruder Detection software, Login Monitoring software, Internet Usage Monitoring software, and Vulnerability & Penetration Testing software.
 4. E-Mail. This procedure should address rules relating to e-mail usage to prevent malicious software, viruses, Trojans, or Worm program script downloads, disguised in a form of an attachment
- C. The protection from malicious software, viruses, and breaches in security that needs to be provided involves reasonable protection from programs or program scripts that may harm Polk County Government's information system.

Instructions for developing and implementing protection from malicious software, viruses, and breaches in security may include:

1. Documentation from software vendor delineating protection provided by the vendor.
 2. Installation of commercial products such as virus protection, intruder detection, login activity monitors, application use monitors, or firewalls.
 3. Continual updating of any commercial malicious software protection and monitoring to determine that it is functional and equipped with the most current revisions and protection updates.
 4. Do not allow opening of any files or macros attached to email that look unusual or are from an unknown source. These attachments should be deleted and the trash emptied.
 5. Delete and do not forward infected, spam, chain or other junk e-mail.
 6. Do not download files from an unknown source
 7. Scan all optical, digital, and magnetic media for viruses before using
 8. Do not upload information from any portable data device, whether connected via USB, Serial, Parallel, Docking Station, or Wireless without examining for malicious software, viruses, or breach of security programs or program scripts.
- D. The Information Technology Department, in coordination with Department Heads, or Division Supervisors, will be responsible for development and implementation of security reminders in compliance with requirements of protecting Polk County's information systems, and HIPAA Security Rules. Security Awareness reminders and training may include:
1. Providing reminders to workforce members to reinforce that security safeguards are in place to protect electronic health information (EHI).
 2. The security reminders will be provided quarterly or as deemed necessary by the Department Heads and / or Division Supervisors, Privacy Officer, or Information Technology Department

3. Place reminders in the facility's regularly distributed newsletter or memo (written or electronic)
 4. Post reminders at specific sites of potential security breach such as fax machines, reception desk, workstations, record storage areas
 5. Add reminders to Agenda topics at regularly scheduled facility meetings, or in training sessions
 6. Display reminders in the form of easily accessible formats such as pens, posted notices, posters, or signs through out the facilities
 7. Post reminders in the form of computer pop up messages
- E. The Information Technology Department, in coordination with Department Heads and / or Division Supervisors will be responsible for training the EPHI workforce, as well as countywide employees on Security Awareness, through formalized training sessions.
- F. The Information Technology Department, in coordination with Department Heads and / or Division Supervisors will be responsible for maintaining the required documentation relating to the provision of security reminders in compliance with the Security Rule. The Privacy Officer will maintain the documentation for at least six years from the date of creation.