STATE OF ALABAMA

Information Technology Policy

POLICY 674-01: VIRUS PROTECTION

Viruses can infect IT systems by a wide variety of methods including e-mail messages, the Internet and through accessing infected files on USB drives, floppy disks, and CDs. Viruses can propagate very quickly as they are easily spread to other network-connected devices. It is vitally important that all IT systems have anti-virus software installed, operational, and up to date to provide real-time protection to the State's network infrastructure and data.

OBJECTIVE:

Protect the State of Alabama computing environment from viruses and other malicious logic.

SCOPE:

This policy applies to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

RESPONSIBILITIES:

Agency Management, Information Technology Organization:

Employ malicious code protection mechanisms (e.g., anti-virus software) at information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers) and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- Transported by e-mail, e-mail attachments, web accesses, removable media, or other common means
- Inserted through the exploitation of information system vulnerabilities

Employ spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.

System Administrators and/or IT Managers:

Develop written operational procedures describing how to handle infected files, how to clean infected systems, and how to verify systems as virus free.

Ensure all files introduced onto computers and all incoming files from external sources, including e-mail attachments, are virus checked.

Update (automatically whenever possible) AV software with the most current virus definitions and apply program updates on all devices that provide AV services.

Ensure system users cannot disable AV software.

Refer to applicable State IT Standards for additional AV software configuration and use requirements.

Update spam protection mechanisms and signature definitions when new releases are available (in accordance with organizational configuration management policy and procedures).

SUPPORTING DOCUMENTS:

- Information Technology Standard 674S1: Virus Protection

By Authority of Director, Information Services Division, Department of Finance

DOCUMENT HISTORY:

Version	Release Date	Comments
670-04	12/12/2006	Original document
670-04_A	3/22/2007	Moved AV program requirement to AV Standard and portable media requirement to Standard 680-01S3
670-04_B	4/17/2008	Removed daily scan requirement; added virus response procedures requirement
674-00	09/01/2011	New document number and format
674-01	11/04/2011	Added Spam Protection responsibilities and link to new Procedure; modified anti-virus responsibility (stated IAW NIST 800-53)
674-01_A	3/14/2017	Deleted link to Procedure 674P1: Spam Protection; procedure is rescinded.