Virus Protection Policy

Objective

The principal concern of this computer virus protection policy is effective and efficient prevention of network virus outbreaks and network security attacks involving computers associated with Auburn University. The primary focus is to ensure that Auburn University-affiliated users (faculty, staff, and students) are aware of and take responsibility for the proper use of the University-provided and OIT-supported virus protection software. This policy is intended to ensure:

1. the integrity, reliability, and good performance of University computing resources;
2. that the resource-user community operates according to a minimum of safe computing practices;
3. that the University licensed virus software is used for its intended purposes; and
4. that appropriate measures are in place to reasonably assure that this policy is honored.

Policy

Centrally provided virus protection software will be run on all Auburn University computers and on all computers connected to the Auburn University Network.

A management structure and supporting guidelines and procedures has been defined and will be utilized by the Virus protection Committee to implement the above policy and ensure compliance.

Virus Protection Management Structure and Supporting Procedures

Goals

- Prevent all infections. And when that is not possible, create an outlet for notification and annotation of virus outbreaks for University service providers and end-users so that future breaches can be prevented.
- Prevent the loss of information/data and software on University-owned computers and computers in the University community and minimize the cost of computing maintenance and network downtime by virus outbreaks.
- Establish and provide authority for a University Virus Protection Committee (VPC).
- Create, train, motivate, and empower a Virus Protection Team (VPT) to implement virus protection software, to monitor virus outbreaks, for computers associated with AU.
- Distribute updates of virus protection software and other important campus-supported software to all University-affiliated computer users. Virus protection software that is not used cannot prevent infections.
- Create a system for automatic, immediate notification of the VPT and the AU user community once an outbreak has been detected.
- Annually evaluate the number of virus outbreaks to determine whether this policy and the University-provided virus protection software are still valid and appropriate.

- Provide and continue to support the best virus protection solution that the Auburn University campus can support.
- Require a minimum of end-user responsibilities in regard to computer virus protection practices.

Compliance

Virus protection is most effective if every computer on the Auburn University network has anti-virus software installed and is actively monitoring network activities. The Virus Protection Team will 1) provide the initial setup for campus computers; 2) distribute virus protection updates. The anti-virus software will be available for AU-affiliated users to install on computers on the campus network or located off campus. The VPT will provide assistance in removing existing anti-virus programs from campus computers.

Service providers will monitor network activity and initiate appropriate action to control infection. Service providers have the responsibility to disconnect any server or client known to be an infecting agent. A "best effort" approach will be instituted to notify the machine owner prior to any disconnection. Such a disconnection is an emergency action.

The service providers or end-user will be contacted immediately, and OIT will work with the service providers and/or end-user to solve the problem. In the case of student-owned machines, the Student PC Shop (SPCS) is available.

Virus Protection Committee (VPC)

Purpose

To administer virus protection policy maintenance and implementation.

Composition

Three faculty nominated by the University Academic Computing Committee (tenure - two years); two students nominated by the SGA (tenure - one year); two professional IT staff nominated by the Computer Support Professional Group (tenure - three years); one OIT staff member nominated by the Executive Director of OIT (tenure - unlimited). The Committee chair is to be determined by the committee.

Responsibilities

- Provide campus-wide leadership in selecting the appropriate anti-virus software for use by the University.
- Annually evaluate the number of virus outbreaks to determine whether this policy and the University-provided anti-virus software and protection measures are still valid and appropriate.
- Recommend changes to this policy and operating guideline as needed.
- Establish and define the authority and responsibilities and oversee the activities of the Virus Protection Team.
- Establish and maintain the criteria needed to become a Registered Service Provider (RSP) of information technology.

- Maintain a list of RSPs.
- Review policy compliance by RSP and make recommendations to the functional head of each provider as needed.
- Designate VPC agents that are qualified to perform virus disinfection, and issue virus removal certification. RSP will be considered VPC agents.

Virus Protection Team (VPT)

Purpose
To provide a University-wide team to manage anti-virus and to serve as a rapid reaction team to manage virus outbreaks.

Composition
One representative from each registered IT service provider (including each unit with OIT designated as such), two representatives-at-large from OIT as nominated by the Executive Director of OIT, the chair or a designate of the VPC, two members-at-large nominated by the VPC. The Team chair is to be determined by the Team.

Responsibilities

- Implement the virus protection policy.
- Coordinate the initial installation of the anti-virus software (and the removal of existing anti-virus software) campus-wide.
- Establish and maintain a communication mechanism providing rapid and effective communication between Team members.
- Establish and maintain a formal virus alert system for notifying the campus community of virus outbreaks and recommend measures to be taken.
- Serve as a rapid reaction team in the event of a virus outbreak.
- Monitor anti-virus software levels and virus infections and initiate defensive action when necessary.
- Monitor and report any virus-related news.
- Analyze virus protection effectiveness and provide a formal report to the VPC by August 31 of each year.

Registered Service Providers of Information Technology (RSP)
Registered Service Providers (RSP) of information technology are personnel who maintain any IT-related service for AU faculty, staff, and students. At Auburn University, a service may be thought of as any production server, any software distribution channels that exist, and any other services provided by the University to users that have the potential for infection and dissemination of viruses. IT service providers are to be registered with the VPC for the purpose of coordination and enhanced communications.

OIT is considered the top level RSP for anti-virus policy and implementation. OIT will be responsible for maintaining the primary software distribution server dedicated to the administration of virus

protection policies and procedures on users' computers. OIT will work in a positive, inclusive manner with other IT service providers.

Responsibilities

- Acquire the licenses for anti-virus software that have been decided on by the VPC for use by the University.
- Procure software and updates from the vendor as they are made available.
- Expeditiously make the software and updates available to AU service providers and users.
- Configure software for distribution in accordance with current AU policy.
- Provide "raw" or un-configured software as needed by other RSP's.
- Provide methods for server administrators and users to update their anti-virus engine and definition files on their own at regular intervals.
- Provide leadership to AU service providers and users.
- Provide documentation for service providers and users.
- Provide requisite instruction for service providers for efficient, effective installation and maintenance of purchased anti-virus software.
- Provide end-users with information on how to acquire the current anti-virus software and, how they work, and how to use them.
- Provide a central repository of information regarding infections by viruses of University owned computers allowing effective reporting and analysis.

Registered Service Providers

Registered Service Providers are responsible for system, site, or network administration server(s) configured with the intention and purpose of regularly providing services including e-mail (SMTP), FTP, Web hosting (HTTP), file sharing, or other services to multiple users (OIT inclusive).

An RSP, in consultation with OIT, can assume some or all end-user support responsibilities herein assigned to OIT. Once these responsibilities are assumed by an RSP, OIT is relieved of the responsibilities until such time as the RSP relinquishes those responsibilities, with the consent of OIT, or fails to shoulder the responsibilities adequately as determined by the VPC.

Registered Service Provider Responsibilities

- Install and maintain anti-virus software on the servers that they manage. The administrator will determine the appropriate level of scanning (on-demand vs. active) based on the performance capacity and purpose of the server. At a minimum, on-demand file scanning must be installed and run on a frequent and regular basis. Administrators are encouraged to install active scanning, but are not required to do so at the expense of general server performance. In addition, administrators of SMTP servers will install email attachment filters, if available, to intercept well known viruses.

- Ensure that they fully understand the configuration and operation of anti-virus software. They will seek assistance or training from OIT or other administrators when questions arise about the proper functioning of software. If contacting the vendor becomes necessary, this will be done through appropriate channels as specified in the license agreement.
- Maintain log files and other records of virus scans. Administrators will rotate logs on a regular basis and will retain old logs and records for a period of one year.
- Notify the owner of the infected file and other RSP's as soon as possible so action can be taken to prevent further infection when viruses are detected on a given server.
- Submit annually a report to the VPC that details the number and nature of virus incidents as well as the steps taken to remove the viruses.
- Upon finding a computer propagating a virus, immediately notify the end-user responsible for the system requesting that the suspect computer be shutdown. If the end-user is not found within three working hours, the computer system can be removed from the network to prevent further propagation.
- Schedule PCs suspected of harboring a virus for disinfection by VPC agents. (Note that some VPC agents may charge for the services provided.)
- Reinstate to the network computers for which the VPC agent has confirmed the disinfection and the virus protection software is current. The VPC agent will report the vital information regarding the infection to the VPT.

Noncompliance
Registered Service Providers, including OIT, are responsible for making the computers and servers under their care compliant with the virus protection policy.

Any system determined to be an infecting agent must be taken off the network or the infection effectively eliminated by the responsible service provider. OIT has the authority to disconnect such an infected system from the network until the infection is effectively eliminated if the responsible service provider fails to manage the infection in a timely manner.

Student-owned computers connected to the campus network must run anti-virus software. The anti-virus software should be active at all times. The student is responsible for keeping the computer system compliant with this virus protection policy.

IT Service Providers Responsible for File Sharing Servers
The protection of servers providing file sharing to client computers is particularly critical to minimizing the spread of viruses. Though viruses are often spread by email, the most rapid and often the most difficult to contain virus outbreaks are spread via shared file systems.

IT service providers providing file-sharing services have a heavy responsibility to be certain that the shared file systems are well protected. Server-based virus protection software that actively scans for all files written to the shared file systems typically causes significant delays in server responses making such active scanning on servers impractical and thus not required for compliance under this policy. Timed virus scanning on servers is required and will catch many of the less virulent strains before they propagate.

Some of the worst viruses to-date propagate much too quickly for timed scans to be effective. Active scanning of files being read from or written to shared network drives is the only means of protection against these virus strains.

IT service providers offering file-sharing services can, therefore, specify virus protection regiments beyond this policy for any users connecting to their file shares. This policy provides IT service providers the right to enforce such regimens. Individuals required to adhere to virus protection regimens beyond those stated in this policy who feel the requirements onerous, should file a formal appeal to the service provider with copies to the service provider's supervisor or director and the VPC.

End-Users

Computer systems owned by Auburn University will run anti-virus software, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy. If a computer has multiple users, none of whom are considered the "primary" user, the department chair or a designee is responsible for compliance. The VPC CSC will consider servers not administered by an RSP, as end-user computers. If no primary user can be identified, the department chair or designee must assume the responsibilities identified for end-users. Computer systems, which provide services (e.g. email, Web hosting, FTP) but are not registered with the VPC, are considered under this policy as "end-users" computers.

Responsibilities

- Install and maintain current virus protection software
- Be certain that the software is running correctly. If these responsibilities appear beyond the end-user's technical skills, the end-user is responsible for seeking assistance from an RSP.
- Initiate disinfecting procedures or seek assistance from an RSP.
- Notify an RSP if a virus infection occurs even if the virus has been successfully disinfected. This information is vital to making others aware of the danger and keeping accurate records of outbreaks.
- Perform regular backups. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible.

Noncompliance

AU faculty, staff, and students not complying with this computer security policy leave themselves and others at risk of virus infections which could result in

- damaged or lost files
- inoperable computer resulting in loss of productivity
- risk of spread of infection to others
- confidential data being revealed to unauthorized persons

An individual's non-compliant computer can have significant, adverse effects on other individuals, groups, departments, or even whole colleges. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

University-Owned Computers
A service provider upon finding a non-compliant computer will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email and a copy of the notification will be sent to the chair of the VPC. The service providers will follow-up the notification to be certain that the individual received and understood the notification. The service provider will provide assistance as needed for the individual to gain compliance.

Faculty, Staff, and Student - Owned Computers
A computer system owned by a faculty, staff member, or student which is on campus and is directly connected to AU Net will be treated the same as a University-owned computer (see section above).

Support for End-User Computers
This virus protection policy includes Windows-based, Macintosh, Solaris, and Linux operating systems. OIT will give priority support for client computers running Windows-based operating systems because 98% of all virus and worms specifically target Windows-based computers. Hence computers running the Macintosh, Solaris, and Linux operating systems are likely to be less well supported.

Individuals who use Macintosh, Solaris, and Linux operating systems will be provided with a copy of the University-supported anti-virus software for their particular operating system. Solaris and Linux users are encouraged to seek publicly available or commercial firewall software from a reputable source, use TCP wrappers and/or employ OS hardening methods to their system.

Distribution
The top level RSP, OIT, is responsible for distributing the software for initial installation and subsequent updates. Although the distribution mechanism depends in part on the specific virus protection software acquired by the University, most include the following distribution methods:

- scheduled, unattended updates by the client via FTP, Web, or propriety agent.
- attended updates initiated by the user of the client via FTP, Web, or propriety agent.
- scheduled, unattended updates initiated by the server via FTP, Web, or propriety agent.

Unless there is a compelling rationale otherwise, all updates will be scheduled. Further, if distribution mechanisms allow, updates will be initiated by the server providing the highest level of protection. Server-initiated updates will normally be timed; however, in the event of a virus outbreak, updates can be pushed to client computers without intervention by the user of the computer.

Definitions

Anti-virus policy server	server that is dedicated to the administration of anti-virus policies and procedures on client computers.
Anti-virus software	software package that is licensed and maintained by Auburn University for use by all University-affiliated faculty, staff, and students in protecting information technology resources both on and off campus.
AU-affiliated user	Auburn University faculty, staff, or student.

AU Net	Auburn University network.
Client	desktop or laptop computer connected to a network.
End-user	individual affiliated with Auburn University as a faculty, staff, or student.
FTP	file transfer protocol.
IT	Information Technology (includes instructional technology).
HTTP	Hypertext Transport Protocol, protocol used by Web browsers to communicate with web servers.
Log files	detailed list of a system's or application's activities. A log can be useful for keeping track of computer use and emergency recovery of data.
Linux	Open source operating system similar to Unix.
OIT	Office of Information Technology for Auburn University.
Registered Service Provider (RSP)	staff employed by OIT or other University divisions whose responsibilities include system, site, or network administration. Registered Service Provider's (RSP's) meet the criteria established by the Virus Protection Committee to provide the IT service and act as agents for the Virus Protection Committee.
Server	computer configured with the intention and purpose of regularly providing services including e-mail (SMTP), web hosting (HTTP), file sharing, or other services to multiple users typically at a departmental or larger level.
Service provider	staff employed by OIT or other University divisions whose responsibilities include system, site, or network administration. Service providers may be registered agents of the Virus Protection Committee.
SMTP	Simple Mai Transport Protocol, protocol used to relay email across the internet.
Virus definition files	Files containing known computer virus definitions used by virus protection programs in scanning for and disinfecting virus outbreaks within computing devices.
Virus Protection Committee Agents	registered service providers (RSP) designated by the Virus Protection Committee (VPC) to disinfect computers.
Virus Protection Committee (VPC)	committee that protects the integrity of the Computer Virus Protection Policy and oversees the implementation of the anti-virus software by the Virus Protection Tam (VPT).

Virus Protection Policy	the policy described in this document for the implementation of an anti-virus software for Auburn University.
Virus Protection Team (VPT)	representatives from each registered service provider and OIT who manage and maintain the anti-virus software and respond quickly to virus outbreaks. The team reports to the Virus Protection Committee (VPC).