

## Departmental Computer Security Policy:

**Background on Issues.** The University has recognized that computer viruses, spread through e-mail, downloads from websites, or sharing of files, represent a major threat to campus computing. CIS provides software tools for virus protection of Windows Systems and Macs and for periodic Live Updates of networked computers. CIS has also announced its policy to isolate from the campus network individual computers and even entire Departments which are identified as sites of virus attacks or from which virus or other computer attacks are being launched. Each Department is expected to be responsible for computer security for those computers under its control.

**Department Policy.** Consistent with this policy, the Department asserts that the following policies be henceforth applied to every computer system on the Department's network whether owned by Brown, an individual, or any other entity.

It will be required that all Windows Systems and Macs used within the Geological Sciences and Chemistry Departments be running Virus Protection software distributed by the University which is regularly updated with the latest virus definitions. These systems must be upgraded with the latest security patches in a timely manner. Instructions will be placed on the Department web site to assist the user in both of these processes. The Administrative passwords to all Windows and Mac systems must be made known to Bill Collins in Geological Sciences, and to Maggie Friedfeld in Chemistry. The DCCs of the Departments, i.e. Bill Collins and Maggie Friedfeld, will have administrative rights on all Cs and Mac systems within their respective Departments.

All unix computers within the Departments must be centrally administered. At this time the administrator is Margaret Doll or her designates for the Geological Sciences Department, and Margaret Doll for the Chemistry Department. The unix systems must be configured in compliance with "The 60 Minute network Security Guide" published by the Systems and Network Attack Center (SNAC) of the National Security Agency. This includes the installation of applicable operating system and application security patches and updates within seven days of their availability on the vendor's web site. These systems will limit outside access via TCP/IP services, and have secure shell installed. TCP/IP services include finger, ntalk, ftp, telnet, rexec, rlogin, and rsh. Sendmail will only run on a limited number of these unix computers.

**To implement this policy, the following procedures are effective immediately:**

- 1). Department Computer support personnel will not be responsible for the maintenance or repair of the software, operating system, or hardware on any Windows System or Mac within the Department that does not have the virus protection software approved by the University running on their system updated with the latest virus definitions. Department Computer support personnel will not maintain or repair the software, operating system, or hardware on any unix computer which cannot be upgraded to a secure operating system as defined in the paragraph above unless alternative security measures which are approved by the central computer administrators have been put in place.
- 2). Systems not protected from viruses or not having the required security patches will not be backed up through the Departmental backup services.
- 3). Computers, including Windows systems, Macs, and unix systems which have been identified as lacking the required virus protection and/or security patches will be denied access to the network.

4). Any user desiring help in identifying the adequacy of the current level of protection on their computer(s) should contact the appropriate DCC for assistance.

5). Assistance will be provided by the DCCs to bring a system into conformance with departmental policy on an "as time permits" basis.