

AUP - Security

Acceptable Use Policy – Security

Security of Information Storage and Transmission

Valparaiso University assumes users are aware that electronic files and transmissions are not necessarily secure.

Users of electronic mail systems should be aware that electronic mail in its present form is generally not secured and is extremely vulnerable to unauthorized access, modification, and forgery.

Users of the World Wide Web should be aware that information sent or received via the Internet is not necessarily secure. Moreover, many Internet sites collect information about the source of inquiries, and some store markers (known as “cookies”) on the user’s computer system for later retrieval by their site or other sites. It is possible for software on a World Wide Web site to explore and retrieve information from the user’s computer without the user being aware of the invasion.

Anyone who “downloads” software, certain applications, or certain file types (such as Microsoft Word documents) should be aware of the possibility that such material could incorporate viruses, worms, or other destructive materials.

Protecting Your Computer Accounts

- Select obscure passwords. Passwords should be at least 8 characters and contain a combination of letters and numbers or special characters but no spaces. Birth dates, social security numbers, and other identifying information do not make secure passwords. Various IT publications provide more information on password security and give instruction for changing passwords.
- Change your password(s) regularly, and at any time you believe it (they) may have been compromised. IT requires all users to change passwords at least every 180 days on IT-managed systems.
- Do not share your login id(s), password(s), or other types of authorization with others.

Protecting From Viruses, Worms, Etc.

- Download materials only from reliable sources.
- Scan for viruses whenever you introduce new software or documents to your computer. IT has a campus license for Sophos Anti-Virus, and routinely scans its servers and IT-managed workstations. This, or other anti-virus software, is a part of IT software installation on any University-owned workstation.

Version	Date	Comment
Current Version (v. 4)	Sep 14, 2017 17:48	Unknown User (rklein)
v. 3	Sep 14, 2017 16:50	Unknown User (rklein)
v. 2	Sep 14, 2017 16:37	Unknown User (rklein)
v. 1	Sep 14, 2017 16:37	Unknown User (rklein)