

Acceptable Usage Policy

Venus Server

1.0 Overview

The Instructional Technology Department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Atlantic Cape Community College's established culture of openness, trust and integrity. The Instructional Technology Department is committed to protecting Atlantic Cape's students, staff and faculty and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

The purpose of the Venus server is to provide students and faculty with an Internet web server for course assignments and instructional resources. This server is to be used only for this purpose and for no other reasons.

Effective security is a team effort involving the participation and support of every Atlantic Cape student and faculty member. It is the responsibility of every Venus server user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of the Venus server at Atlantic Cape. These rules are in place to protect the students and faculty of Atlantic Cape. Inappropriate use exposes Atlantic Cape to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to students, faculty members, and support staff at Atlantic Cape, including all personnel affiliated with third parties. This policy applies to all services supplied by the Venus server.

4.0 Policy

4.1 General Use

While the Venus server administration team desires to provide a reasonable level of privacy, users should be aware that the data they store on the Venus server remains the property of Atlantic Cape. Because of the need to protect the Venus server, management cannot guarantee the confidentiality of information stored on the Venus server.

Students and faculty are responsible for exercising good judgment regarding the reasonableness of personal use. At no time shall the services on the Venus server be used for personal use. If there is any uncertainty, students and faculty should contact the Instructional Technology department at Atlantic Cape.

For security network maintenance purposes, individuals authorized by Atlantic Cape may monitor equipment, systems, and network traffic at any time, per the InfoSec's Audit Policy.

Atlantic Cape reserves the right to audit the data stored on the Venus server to ensure compliance with this policy.

Students are provided with three hundred megabytes of space initially on the Venus server. If additional space is required, a student should contact their instructor for their course.

Student data placed on the Venus server will be available for up to one year after the student has enrolled in a course requiring web access. Students are responsible for backing up content on the server before this time elapses.

4.2 Security

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

All access to the Venus server should be done through an authenticated and encrypted connection. Acceptable access methods can be HTTPS WebDAV and S/FTP. If there is any uncertainty regarding the access method a student or faculty member is using, contact the Atlantic Cape Instructional Technology department.

If any time you feel there has been some form of unauthorized access to your account, please contact the Atlantic Cape Instructional Technology department.

4.3 Acceptable Usage

The following represents examples of Acceptable Usage for both students and faculty for using the Venus server.

- Websites based on course assignments. This data can represent HTML files, interactive media, pictures, and all other content necessary for course assignments.
- Classroom resources such as PowerPoint presentations, syllabuses, homework assignments, and others.

- Any other content approved by an instructor of a course or by the Atlantic Cape Director of Instructional Technology

4.4 Unacceptable Usage

The following activities are, in general, prohibited. Employees may be exempted from these restrictions only if these activities are approved in writing by the Atlantic Cape Director of Instructional Technology.

Under no circumstances is a student or Atlantic Cape faculty member authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing the services provided by the Venus server.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Atlantic Cape.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Atlantic Cape or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the Venus server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the services provisioned by the Venus server to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.
- Making fraudulent offers of products, items, or services originating from the Venus server.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee

is not an intended recipient or logging into the server or account that the student or faculty member is not expressly authorized to access. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, any form of denial of service, and forget routing information for malicious purposes.

- Port scanning or securing scanning is expressly prohibited unless prior notification to the Atlantic Cape Director of Instructional Technology is made.
- Circumventing user authentication or security of any host, network or account.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet.
- Providing information about, or lists of, Atlantic Cape students and faculty to parties outside Atlantic Cape.
- Using the services provided by the Venus server to ascertain any personal or financial gain.
- The placement of any adult only content onto the Venus server is strictly prohibited.

5.0 Enforcement

Any student or faculty that is found to have violated this policy may be subjected to disciplinary action, up to and including termination of their account.