

ELIZABETH CITY STATE UNIVERSITY
Abusing, Damaging or Destroying Electronic Resources

I. Purpose

The purpose of this policy is to outline certain behaviors and/or acts that Elizabeth City State University does not tolerate, and to articulate how the institution will respond when incidents of abusing, damaging or destroying electronic resources are reported.

II. Scope

This policy applies to all personnel who include full time regular, temporary and part-time employees, full-time and part-time students, contractors, and all other authorized users of any University Information Systems, including University-hosted, third-party hosted, and Internet Service Providers (ISP).

III. Policy

Users are encouraged to make use of the University's computing and communication resources in pursuit of legitimate activities that further the educational, research, administrative, and service mission of the institution. However, users must also be aware of the finite capacity of computers or network systems, and of the resources required to obtain and support those resources. Such resources are shared among all members of the campus community, and it is in the interest of all users to ensure the proper functioning, availability, and performance of computing and communication systems and networks. Damaging, abusing, or in other ways destroying or interfering with the successful operation of electronic computing and communication resources is forbidden. Users must take care not to engage in activities that, without proper authorization:

- A. Overload the computing systems and networks, such as excessive use of processor time, data storage, or bandwidth, or activities which otherwise impair or negatively impact performance and availability;
- B. Interfere with, disable, damage, obstruct, or in similar manner impede the normal function and accessibility of computer or communication systems, or computer data, files and other information;
- C. Waste or hoard computer or network resources in ways that interfere with the operation of the system or its availability to others;
- D. Attempt the unauthorized connection, removal or modification of computer or communication devices;
- E. In any way physically abuse, damage, or destroy computing or communication systems, data, or facilities;

- F. Disseminating or launching any executable program designed to damage systems or data, or place excessive load on a computer or network affecting its performance or availability.

IV. Violations of Policy

Violation of this policy may constitute misconduct and accordingly employees are subject to disciplinary action, up to and including suspension without pay and dismissal, in accordance with the pertinent employment policies for SPA, EPA non-faculty, and faculty.

Sanctions for violation of this policy may include suspension or revocation of access privileges in addition to any other sanction permitted under the Student Code of Conduct.