CHAPTER 700

INFORMATION TECHNOLOGY
ELIZABETH CITY STATE UNIVERSITY
Web Page Policy

1. Purpose of Policy

The World Wide Web allows Elizabeth City State University staff, faculty, and students to promote university educational opportunities and activities to a local, regional, and international community that includes alumni and current and prospective students, faculty, staff, and friends.

2. Structure

a. Elizabeth City State University’s World Wide Web pages are considered university publications as well as campus-wide information sources. The web administrator oversees the structure and development of the Elizabeth City State University main home page and determines the guidelines for consistent graphic design, writing style, and accuracy of official information for the home page (located at http://www.ecsu.edu) and the pages linked directly to it.

b. The Academic Computing Center provides the computer hardware and access to Elizabeth City State’s main web server.

c. Various areas of the university also maintain web servers, using university equipment and staffing. This policy applies to any Elizabeth City State University web server, web server administrator, web server page owner, or web page publisher.

d. Server space

1) General principle: Elizabeth City State University does not grant unique domain names that are not a variation of the www.ecsu.edu domain name.

2) General principle: Any individual or organization receiving Elizabeth City State server space must abide by all university guidelines, including the university’s web policy.

3) Any individual or nonprofit organization that receives funds through the university (i.e., anyone who has a letter of agreement with Elizabeth City State University) may receive server space. If support is requested, the individual or organization will be notified that such service is not guaranteed and, if provided, will be treated as a low priority for the server staff.

4) Professional, nonprofit organizations sponsored by a member of the Elizabeth City State University community, whose mission is directly tied to the university’s mission, may qualify for server resources. Resources may be provided only if these resources do not have a negative impact on server efficiency. The faculty or staff member affiliated with the organization will be responsible for developing and maintaining the page, with no support from the server staff. Any faculty or staff member requesting server space must submit a
5) written request to the ACC and must state how the mission of the requesting organization is tied to the university’s mission.

6) Acquiring server space does not guarantee a link from an official ECSU web page, nor does it imply that the server space holder will receive a requested uniform resource locator (URL).

7) Professional, nonprofit organization files will reside in the web directory of the affiliated member (who also is an ECSU faculty or staff member).

3. Official and Unofficial Web Pages

The Elizabeth City State University web site includes both official and unofficial pages. Official pages are those of university offices or departments sanctioned by the Chancellor of ECSU or his designee. Unofficial pages are those not sanctioned by ECSU, including but not limited to faculty, staff, and student personal pages and student or employee organization pages.

Elizabeth City State University is not responsible for unofficial pages. The university reserves the right, however, to remove from any Elizabeth City State web server any page that is found to be in violation of the law or university policies or interests or that is detrimental to performance of the web server or the network.

4. User Responsibilities

a. The names, initials, seals, mascots, and logos associated with Elizabeth City State University are trademarks owned by the university.

b. Elizabeth City State University web page owners and publishers are responsible for the content of their pages and are subject to all university policies and standards pertaining to print publications and computing ethics.

c. Without specific authorization from the web administrator, Elizabeth City State University web servers may not be used for the following:

Advertising or server space for non-university or organizations.

A web advertisement consists of:

- Text or graphics placed on a web page that have been paid for by a non-Elizabeth City State University organization; or,

- Text or graphics placed on a web page in exchange for goods or services.

The following examples do not constitute an advertisement:
5. Guidelines for Official Pages

Web page owners are responsible for presenting accurate data and for updating any material they publish on the university’s web servers. Page owners and publishers who maintain official ECSU web pages must adhere to the following publishing guidelines:

- Create a visual heading for the top of the page, which clearly identifies it as an ECSU College, school, department, program, area, etc. Include the <title> tag and a title for the page within the <head></head> tags for the indexing/search purposes, such as:

```
<HEAD>
<TITLE>Elizabeth City State University’s Home Page</TITLE>
</HEAD>
```

- Include the name and e-mail link of a faculty or staff contact person or departmental e-mail address at the bottom of each page (an e-mail link must not be a student e-mail address).

- Note the date the page was created or updated (if more than one person is maintaining the page, the author may want to include the name or initials of the person who made the last modification).

- Link each page to one or more previous pages; include a link to the Elizabeth City State University home page at [http://www.ecsu.edu](http://www.ecsu.edu) on the area’s “top-level page”.

---

- General interest links to commercial web sites that may be of interest to web viewers and that are available free of charge (e.g., links to Alta Vista search service, Elizabeth City home page, area weather links);

- Subscription services or site licenses for which the university pays, in order to gain access to a commercial service (e.g., Netscape Navigator);

- Information that relates to or supports the teaching, research, or service mission of the university, such as academic departmental conferences; or,

- Listings of sponsors for a performance or special event (The listing must not be hyperlinks to a commercial sponsor’s web page).

- Activities that would provide non-university related persons or organizations monetary gain; or,

- Activities that would provide direct financial benefit to any non-Elizabeth City State University organization.
Create text alternatives for graphics so those users who are unable to view graphics will understand the page and be able to navigate it.

Ensure that pages are not created in ways that prevent users of text-based browsers and people with disabilities from accessing or navigating the web.

Respect the copyrights of text, sound, and graphic material, remembering that the appearance of material in print does not indicate that the university holds permission for use beyond that appearance.

Commercial Links

1. Elizabeth City State University web pages can provide a text link to a commercial site if the university has an exclusive contractual relationship with the business. Logo links are not permitted on university pages unless the web administrator grants an exception.

2. Elizabeth City State University web pages can provide a text link to a commercial site if the site provides a service to the university’s primary community (faculty, staff, or students), as long as the university is not receiving any goods or services for creating the link.

3. Elizabeth City State University web pages will not link to the site for any commercial web developers who have created the site or the pages contained therein. This principle applies to situations in which the university paid for the service and in which the service was provided free of charge. Attribution can and should be listed, but no links can be provided and no commercial logos displayed.

4. Check pages on a regular basis for dead links and keep information current.

6. Additional Information Regarding Student Organizations and Student Personal Pages

a. Server space is available to any student organization registered with the university.

b. The content of a student organization’s web page must relate specifically to the activities of that organization. Organization pages must include the campus address and phone number of the organization or the name of a responsible officer.

c. Space allocated to an organization may not be used for personal pages of members or officers of the organization. However, an organization page may provide links to personal pages. If links are provided to student personal pages, the standard disclaimer
7. Appeals

a. Appeals regarding any of the guidelines in this policy may be made to the web administrator.

8. Policy Review

a. This policy will be reviewed as needed, at least annually.
ELIZABETH CITY STATE UNIVERSITY
Acceptable Use of Technology Policy for University Employees

Preamble

Elizabeth City State University (ECSU) has critical dependencies upon its computer information systems in order to meet operational, financial, educational, and informational needs. It is essential that ECSU's computer systems and computer networks, as well as the data that reside on and are processed by these technologies, be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access. Federal and state law, and ECSU policies and procedures govern the use of these technologies.

1. Scope of Policy

This policy applies to ECSU computer systems and refers to hardware, software, data, and communications networks associated with these computers. In particular, this policy covers computers ranging from multi-user timesharing systems to single-user personal computers, whether stand-alone or connected to the campus network. This policy governs ECSU employees who utilize these university resources.

2. Regulatory Limitations

A. ECSU may monitor access to the equipment and networking structures and systems for the following purposes:

1. to insure the security and operating performance of its systems and networks;

2. to review employee performance;

3. to enforce international, federal and state laws and university policies.
B. ECSU provides a computer and appropriate software and accessory equipment to employees. Ownership of this property rests solely with the university. Employees have no ownership rights to this equipment or the information sent or received through this equipment. Employees will have no expectation of privacy with regard to this equipment or information. The computing equipment provided to employees, including information sent or received through this equipment, is for university business.

C. ECSU reserves the right to monitor this equipment or audit its use to insure that all usage complies with university rules, regulations and policies, with the laws of North Carolina, with the laws of the United States, and with international laws. To facilitate ECSU’s right to monitor and audit, appropriate university employees may inspect and review this equipment and information sent and received through this equipment at any time.

D. Employees may not use this equipment to harass or stalk others, post, transmit or create any unlawful, threatening, assaultive, fraudulent, defamatory, obscene or pornographic communication or any other communication where the message, or its transmission or distribution, would constitute a criminal offense, give rise to civil liability or otherwise violate any university policy or any state, national or international law.

E. Employees may use this equipment for minimal personal communication as long as this usage does not interfere with the employees’ work obligations, the work of other employees, or the integrity or viability of the equipment or the networks to which it is attached. Furthermore, any usage must not violate other sections of this policy. ECSU may monitor or review employee’s personal use and the information employees send or receive to insure compliance with this and all university policies.

F. ECSU reserves the right to limit access when international, federal or state laws or university policies are violated or where university contractual obligations or university operations may be impeded.

G. ECSU reserves the right to monitor or restrict files or software residing on university computers housed within a private domicile and reserves the right to restrict the installation or copying of university files or software on non-university computers, whether or not such computers are attached or able to connect to campus networks.
H. All material prepared and utilized for work purposes and posted to or sent over ECSU computing and other telecommunications equipment, systems or networks must be accurate and must correctly identify the creator to campus networks.

I. Any creation of a personal home page or a personal collection of electronic material that is accessible to others must include a disclaimer that reads as follows:

“Elizabeth City State University does not endorse, sponsor or provide material located on this site.”

3. Permissible Use

Employees are expected to follow this policy and any related university policies, regulations and procedures for ECSU work produced on computing equipment, systems and networks. Employees may access these technologies for personal uses if the following restrictions are followed:

A. The usage is lawful under international, federal and state law.

B. The usage is not prohibited by The University of North Carolina Board of Governors or university policies.

C. The usage does not overload the university’s computing equipment or systems, or otherwise harm or negatively affect the system’s performance.

D. The usage does not result in commercial gain or private profit (other than allowable under university intellectual property policies).

E. The usage does not violate federal or state laws or university policies on copyright or trademark.

F. The usage does not state or imply ECSU sponsorship or endorsement.

G. The usage does not violate state or federal laws or university policies against race or sex discrimination, including sexual harassment.

H. The usage does not involve unauthorized passwords or identifying data that attempt to circumvent system security or in any way attempt to gain unauthorized access.
4. Violation of Policy

Violators of this policy may be denied access to the campus network. In addition to any possible legal sanctions, violators of this policy may also be subject to disciplinary action up to and including dismissal or expulsion, pursuant to ECSU campus policies, codes of conduct, or other instruments governing the employee’s relationship with ECSU. Recourse to such actions shall be as provided under the provisions of those instruments.

5. Application of Public Records Law

All information created or received for work purposes and contained in university computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records Law applies. This information may be purged or destroyed only in accordance with the ECSU records retention schedule and State Division of Archives regulations.

6. Review

ECSU reserves the right and has the authority to interpret and apply this policy and to modify or amend it at any time. It is imperative that each employee reviews and complies with any changes made to this policy.
ELIZABETH CITY STATE UNIVERSITY

E-Mail Retention Policy

A. Electronic mail or “E-Mail” is simply a method or communicating information and does not constitute a public record in and of itself. However, the information transmitted through the use of E-Mail may become public record if it meets the definition of N.C. Gen. Stat. 132-1 (http://www.ncga.state.nc.us/enactedlegislation/statutes/html/bysection/chapter_132/gs_132-1.html), i.e., if it is information made or received in the transaction of public business by a state agency. If information transmitted by E-Mail meets the definition of “public record”, then it may not be deleted or otherwise disposed of except in accordance with a records retention schedule approved by the State Division of Archives and History. The content of the E-Mail message determines the retention requirement.

B. The individual to whom the message is addressed becomes the legal “custodian” once the message is received and is the person responsible for ensuring compliance with the Public Records Act. Although most agencies also periodically back up information residing on system hard drives this is not done for archival purposes or in order to meet the requirements of the Public Records Act, but as a safety measure in case of system failure or unlawful tampering (“hacking”). The system administrator is not the legal custodian of messages which may be included in such back up files.

C. E-Mail messages generally fall into two categories.

- First, some E-Mail is of limited or transitory value. For example, a message seeking dates for a proposed meeting has little or no value after the meeting date has been set. Retention of such messages in the computer system serves no purpose and takes up space. Such messages may be deleted as soon as they no longer serve an administrative purpose.

- Second, E-Mail is sometimes used to transmit records having lasting value. For example, E Mail about interpretations of an agency’s policies or regulations may be the only record of that subject matter. Such records should not be maintained in E-Mail format, but should be transferred to another medium and appropriately filed, thus permitting E-Mail records to be purged at regular intervals.

D. While the methods for reviewing, storing or deleting E-Mail vary, compliance with the retention requirements of the Public Records Act may be accomplished by doing one of the following:

- Print the E-Mail and store the hard copy in the relevant subject matter file as would be done with any other hard-copy communication. Printing the E-Mail permits maintenance of all the information on a particular subject matter in one central location, enhancing its historical and archival value.
Electronically store the E-Mail in a file, a disk or a server, so that it may be maintained and stored according to its content definition under the unit’s records retention policy.
Elizabeth City State University
PC Replacement Policy

1. When to replace:

Personal computers (PCs) should be replaced when the hardware becomes a barrier to the user. This occurs primarily when the university’s standard software suite, or the software required for instruction, service, or business activity will not run effectively on the existing hardware. In addition, when PCs serve as both an integral component in an educational program as well as a marketing tool for attracting new students, replacement should be considered when the computer can no longer present a positive programmatic image. This may be the case in some of the university’s high tech curricula.

2. The down side of replacing computers:

PC replacement is expensive, disruptive and labor intensive for both the end user and the support staff. Changing computers often requires a migration of data files and ancillary programs from the older units to the new units, and may require relearning software functionality when the newer PC comes in with newer software versions. In addition, newer units may no longer support legacy applications, which can lead to the need to purchase additional software upgrades or system modifications. Further, adding a new computer with new software versions to an existing office or facility can cause problems when shared files are no longer compatible.

3. Guidelines for replacement:

a. In an effort to balance the need to upgrade with the negative effects of replacement, PC purchasing must be orderly and planned in advance. The policy outlined here covers all PCs whether student, faculty, staff or administrative. The following guidelines are offered to assist with replacement planning:

   - PCs should be purchased with enough technical capacity (e.g., memory, processor speed, hard drive space, etc.) to support the user through the entire life cycle in its initial location. The life cycle for all newly purchased PCs in the initial install location should be a minimum of three years and an average of four years. This life cycle should be periodically reviewed. As PCs become less expensive and networking more advanced, shorter life cycles may be practical. In general, the more expensive/advanced a PC, the longer its average initial life cycle should be.

      The selection of the standard computer for each ordering cycle cannot simply be based upon price alone. The selection should seek to balance an increased life cycle resulting from purchasing increased capabilities, against the initial PC cost. Area supervisor’s should also do the same when adding additional optional capabilities.
More frequent replacements, resulting in shorter initial life cycles, require the approval of the Chief Information Officer. In addition, because these result in additional labor costs, data migration and application reinstallation support will not be provided when a PC is replaced after less than three years of use. It is unfair to compromise the normal support needed by other end users, for the extra support needed when PCs are replaced with greater than standard frequency. For these installs, the end user is responsible for the migration of data and the reinstallation of programs. Should the end user be incapable of this task, services can be provided on a low-priority basis.

b. Within the initial life cycle, at most PCs should require only one major software upgrade (operating system or office suite) and should not require a hardware upgrade. If the user’s needs change, necessitating a change in hardware configuration, only one upgrade (RAM, hard disk, processor, etc.) should be scheduled during the equipment’s initial installation. This upgrade should not occur in the computer’s last year at its initial location, unless the upgrade contributes significantly to the utilization of the equipment in its second location.

- Zip drives or re-writeable CD drives may be used to extend the life of a computer, and should be considered an alternative to adding another hard drive. These drives should be used to provide additional data storage, facilitating migration when the PC is replaced.

c. Used PCs should remain in their second location for at least one year. The distribution of used equipment is to be managed by Academic Computing & End User Support Services.

d. PC purchases should be planned so they equip entire facilities/offices during one purchase cycle. Equipment funding should not be provided piecemeal. As an example, rather than appropriating $4,000 a year to a department for a gradual replacement of hardware, the college should provide $16,000 every four years to allow all units to be replaced simultaneously. Note: Departments cannot carry over funds from year to year. Senior Administrators need to plan department and office budgets to support full facility replacement.

- Some office PCs will not have the same software requirements as the rest of the office’s equipment. For example, a PC may be a single function device used by a work study student where compatibility or efficiency of use is not a major factor. Here, a second hand PC or a PC replaced less often may be more appropriate. Supervisors should not automatically replace this equipment when the office’s primary equipment is upgraded but base the replacement on its need for compatibility.

e. For planning purposes, a PC’s projected replacement schedule should be established when initially acquired. This information is to be kept by the Director of Academic Computing & End User Support Services. The area’s tentative replacement schedule should be based upon
the replacement dates for each device. The identification of the specific PCs to be replaced should be based on its functionality and should be established one year in advance.

f. For budgeting purposes, PC replacement should be included as an annual, specifically identified line item in the budgets for each unit/school/department. Funding for these accounts should be based upon a percentage of each area’s new equipment inventory. If the average life cycle of newly purchased equipment is 4 years, the annual replacement plan would cover 25% of the inventory. Reliance on “One Shot” initiatives to catch up should be avoided.

- Replacement ordering will occur within the cyclical ordering cycles set for all university PC ordering.

- Note: Once a PC is replaced from its initial installation, it should not be included in calculating the inventory to be replaced. Only equipment in its initial life cycle should be included here.

- The percentage used for budgeting is to be established after comparing the ideal replacement rate to the university’s funding ability. Each unit/division/school/department will be responsible for developing and managing their inventory.

- PC replacement should not automatically include the replacement of the monitor. Individuals should plan on keeping their existing monitor through two replacement cycles unless the monitor can no longer support the technical needs of the user, or the monitor needs to remain with the replaced PC as it moves to its second location.

g. There are two types of PC purchases—those to replace existing equipment and those to add new equipment. These functions should remain separate. In other words, departments should not buy a new PC to replace an older unit and then plan on handing down the older unit to another user, who will then hand down that replaced unit to another user, etc. This results in multiple installations, multiple end user disruptions, and leads to a break in the orderly replacement schedule for the department. See Item 4 above for preferred purchase planning method.

- To discourage the above practice, when a new PC is purchased as a replacement for an existing unit, the replaced unit should return to campus stock. Here its distribution will be based upon an evaluation of the campus’s overall needs. Units not needed on the campus, may be moved to other locations for secondary uses.

- If an additional PC is needed within a department, the campus should first look to acquire a unit from stock, of the same vintage as the rest of the department’s equipment. The goal is to keep the entire department/facility on its initial replacement schedule and all users on the same software versions.

h. Campus lab replacement should be handled on a staggered schedule such that there is at least one new facility available on a campus at any one time.
Where academic computing centers support the campus’s advanced curricular, the lab should have at least one current area that can provide resources equal to the new facility on the campus.

i. Some classes will require the most current equipment to support their instructional needs. Rather than scheduling more frequent equipment replacements in the lab facilities, these classes have traditionally used, the campus should consider moving the class to the newest campus/building/department facility.

   ▪ In general, the university needs to be less proprietary with labs to optimize utilization. Those functions that work best together could share computer facilities. New labs would only need to be added when the utilization of all existing labs that are capable of supporting the needed function are nearing 100% utilization. It is recommended that the deans consider the shared facility option as the campus plans and develops new lab spaces.

j. Campus cyclical purchasing should include the purchase of a small stock of extra computers. These would be available to fulfill off-cycle requests for needs such as providing equipment for new hires. The stock would be kept current by distributing any unused product from the previous cycle, to individuals requesting machines on the upcoming cycle, and replenishing the stock of spares with the new order.

   ▪ It is expected that all individuals in new positions will need access to computing technology. Upon the creation of a new position, the department, office or campus should include plans to acquire the necessary equipment. When evaluating the PC needs of an individual in a new position, the vice chancellor or department head should consider the age of existing equipment within the area. If possible, equipment of similar vintage should be obtained. If new equipment is appropriate, its acquisition should be included in the purchase cycle prior to the individual’s arrival.

Individuals hired on existing lines are expected to use equipment currently in place.
ELIZABETH CITY STATE UNIVERSITY
Web Accessibility Policy

These Web Publishing Standards apply to the publication of information on the Internet at Elizabeth City State University and particularly to the publication of information on the official ECSU Web Server (www.ecsu.edu). These standards are established and approved by the University’s Web Master.

1. Publishing Information on the WWW.ECSU.EDU Web Server

a. When the updates are ready to be published to the web server, the appropriate authorized personnel will submit a 3.5” disk with all the current HTML or information. Pages with prior authorization will be updated automatically. Otherwise, requested updates will be approved within 1 business day, if they meet the standards outlined in this document. Updates that do not meet these standards will not be approved until they are brought into compliance and resubmitted for approval.

2. Responsible Entities

a. Each web page that resides on the Elizabeth City State University Web Server must have a designated responsible agent. It is the duty of these responsible agents to verify and ensure that each of their web pages adheres to the standards specified in this document as well as the WWW Policy. Pages not currently compliant with these standards must be brought into compliance with these standards within one month of the publication of these standards. If these standards are changed in the future, it will be the responsible agents’ responsibility to bring their web pages into compliance with the new standards within a reasonable period of time. Pages not brought into compliance will be subject to the penalties described below.

3. Official ECSU Web Page Content Standards

a. The standards given below must be adhered to by all web transmitted information offered on the ECSU campus, including, but not restricted to, those pages offered from the www.ecsu.edu web server and any personal web pages offered using the Elizabeth City State University Web Server. Web transmitted information on University owned equipment in violation of these standards is subject to removal. Ports with non-University owned equipment that host web transmitted information in violation of these standards are subject to immediate disconnection from the campus network. Furthermore, if such web transmitted information also violates the University’s official published policies or any federal, state or local laws (e.g. copyright, libel, privacy) the incident may be referred to the appropriate campus department for resolution. Such
cases may result in suspension from the University as well as prosecution by outside authorities. Other penalties described below may be applied as appropriate.

- Official ECSU Web pages will be sponsored by recognized entities of the university (Liaisons). Liaisons may create home pages and other web pages that serve to carry out official University business. The University Webmaster is the Liaison for the top level Elizabeth City State University Home Page.

- Liaisons are responsible for maintaining the accuracy, timeliness and consistency of page content for their respective areas. Pages not meeting this guideline are subject to removal if not brought into compliance in a reasonable period of time. Individuals updating pages who are not designated to do so by the appropriate Liaison will be considered to have committed computer abuse.

- Elizabeth City State University resources may not be used to create WWW pages primarily for personal business or personal gain, except as permitted by other university policies. Violators of this are subject to termination of access to network services.

- Issues of privacy and confidentiality of information will be considered by the University Web Master. In general, custodianship of sensitive records is the responsibility of university offices maintaining such records, and no such records will be published on the ECSU WWW site without permission of the custodian. Violators of this policy are subject to termination of network services for any system(s) on that network jack and referral to the appropriate campus department for resolution.

- Limitation on the size and number of these pages may be imposed in the future if resources become overburdened. Personal pages will be removed when the person in question departs from the university.

- If an individual suspects any violations of University policies, the person should contact the University Web Administrator (webmaster@mail.ecsu.edu).

4. Suggestions

- Make sure all your links work before requesting publication.

- Web page should take no longer than 30 seconds to download on a 28.8 modem.

- Create a visual heading for the top of the page which clearly identifies it as an ECSU, school, department, program, area, etc.

- Include the <title> tag and a title for the page within the <head></head> tags for the indexing/search purposes.
Include name and e-mail link of faculty, staff person, or department (Must not be a student e-mail address), and last updated date at the bottom of each page. Outdated information will be de-linked.

Images used on a web page should relate to and compliment the content.

When using graphics on your page, you are advised to have a “Text Version” in consideration for users with lower version browser and PCs.

Provide a text or graphical navigation bar for each page. Include a link back to the originating page as well as the ECSU Homepage. (www.ecsu.edu)

You can use any of Elizabeth City State University’s logos.

The web page should be no larger than 640x480 pixels.

Refrain from using excessive animated gifs or other bells and whistles because it takes away from the intended message and it slows down the download time.

Design the page around the content.

The content of the web page should be written with the audience in mind. Long textbook descriptions and content should be avoided since it is usually uninteresting. Cut down long-winded text into bite size sections that are logically grouped.

Be mindful of wild backgrounds, which have the tendency of taking away from the text as well as making it hard to read. For long content use the black text on the white background.
ELIZABETH CITY STATE UNIVERSITY
IT Management Flexibility

Introduction

Support of Campus IT Strategic Plan

The primary objective of the IT Strategy at ECSU is to improve the operational effectiveness and efficiency of the university through the use of technology. The planning process for the IT Strategy begins each year when the chancellor has a retreat for his cabinet. The CIO is a member of the chancellor’s cabinet. During this retreat university goals for the upcoming school year are established and prioritized. Each unit then establishes goals and objectives that support the university’s goals and objectives. As the IT goals and objectives are established, the following inputs are used as the university community continues to achieve its IT core mission of “Improving the Operational Effectiveness and Efficiency of the University through the use of Technology”:

- University Goals and Objectives
- User Requirements
- Board of Governor’s Strategy
- ECSU’s Strategic Plan
- UNC IT Strategy
- Shared Services Alliance
- Teaching and Learning with Technology Collaborative (TLTC)
- Distance Learning (e-Learning)

The above factors drive the IT operational plan. Users at ECSU have played and will continue to play a key roll in the decisions such as the need to implement WEB for Students, WEB for Faculty, Alumni Development System (ADS) and our Human Resource System (HRS). Likewise, the strategic direction to migrate from SIS/Plus to Banner was user driven. Individuals from the University are active participants as members of the Board of Directors for the Shared Services Alliance and the Board of Directors for the TLTC. End-user groups meet on a regular basis to address their needs. There are user groups for the respective applications at the campus level and at the university level. The university group has representation from each campus.

The IT Strategic Plan is reviewed and approved by the Information Technology Planning and Policy Council (ITPPC). The information then becomes part of ECSU’s Strategic Plan. The university’s strategic plan is then reviewed and approved by the Administrative Council. The CIO is chairman of the ITPPC as well as being a member of the Administrative Council.
Support of the Campus Strategic Plan

ECSU’s Strategic Plan 2002-2007 contains six institutional goals. The IT plan supports all six goals. The strategic IT goals are given below with an overview of how they support the University’s Strategic Goals.

ECSU Goal #3: The University will attract and retain a highly motivated student body.

The intent of the IT Strategy in support of this goal is to provide state-of-the art technology for students and faculty in the classrooms and the residence halls. Our instructional technology efforts are designed to assist faculty as they integrate technology into the teaching and learning processes. WEB for Students and WEB for Faculty will provide better access to the information that is needed in real time. Students have access from their residence hall rooms to e-mail and the Internet using wireless technology. Campus computer labs are available for use by students, faculty and staff. Training workshops are conducted for faculty, staff and students.

ECSU Goal #5: The university will enhance administrative efficiency and effectiveness of each organizational unit. As a consequence, through continuous human resource development, expanded automation, improved data processing, and state-of-the-art information technology, students, faculty and staff will acquire and use knowledge in advanced technologies, the teaching/learning process and organizational effectiveness.

The intent of the IT Strategy in support of this goal is to improve the operational effectiveness and efficiency of each organizational unit through the use of technology. Each faculty and staff member has been provided with desktop computers that are attached to the campus fiber network. They have access to campus provided e-mail and the Internet. Based on need, access is also provided to host-based applications such as Financial Records System (FRS) and Student Information System (SIS). WEB for Students provides students with the capability to view their transcripts/grades and determine graduation requirements using Degree Audit as well as pre-register/register for classes. They can also access their student accounts and determine their financial status such as how much money they owe the university as well as how much financial aid has been awarded. Faculty can get class rolls and enter midterm and final grades directly into the system. These capabilities provide real time access and they eliminate the need for personnel to provide this type of information over the telephone or for students to visit
the business office, the registrar's office and financial aid. Human Resources System (HRS) is another mainstream application that is used by the Human Resources department and Business and Finance. A new Alumni Development System (ADS) has also been installed. The system will provide improved data management, tracking and record keeping in the Division of Institutional Advancement.

Training workshops are conducted in the Information Technology Center for faculty and staff. These workshops include topics such as basic personal computer concepts, word processing (WordPerfect, Microsoft Word) and spreadsheet (Excel) use, PowerPoint, Internet use, setting up a Website and the use of technology in the classroom. Workshops are often tailored to meet the needs of the targeted group. One-on-one training is also available.

**ECSU Goal #6: The University will broaden its educational and community outreach**

The e-Learning Program (Distance Education), under the direction of the Virtual College, supports this goal consistent with the UNC IT Strategy Focus 2. The Virtual College extends availability and access to on campus courses via distance education to students who are isolated from campus due to time and/or geographic location. The NCREN Center has two classrooms that are equipped for receiving and delivering instruction. One of the classrooms is located in the Information Technology Center. The other classroom is located in the Jimmy R. Jenkins Science Building.

**Support of the UNC IT Strategy**

In 1999 the Board of Governors adopted the University of North Carolina’s Information Technology Strategy. As a result of this strategy, ECSU received additional IT positions and funding to begin the establishment of a state-of-the-art network infrastructure. Through State appropriations and the Bond project for IT Infrastructure upgrade, the university has been able to complete Phase I of the strategy, which addressed minimum wiring standards. Phase II of this strategy dealt with the following focus areas:

- Administrative Systems and Student Services
- Teaching and Learning with Technology (TLT)
- Distance Learning (e-learning)

Our IT strategy is consistent with and supports the goals established by the UNC IT Strategy. We are active participants by holding full membership on the Shared Services Board of Directors. The CIO represents ECSU on this board. The director of Academic Computing & End User support served two terms on the Teaching and Learning with Technology Collaborative. The Director for Center for Teaching Excellence now serves on the TLTC. We are also active participants in UNC CAUSE, NCREN and the Super Computing Advisory Boards.
Below we will address each of the focus areas and give an overview of how ECSU’s IT Strategy supports the UNC IT Strategy:

**UNC IT Strategy Focus 1: Campus Teaching and Learning with Technology** includes instructional technology support and equipment that is needed to integrate technology into the Teaching and Learning Process.

The primary leaders in the TLT effort consist of staff from Academic Computing and the recently established Center for Teaching Excellence, which includes the Virtual College and the NCREN Video Conference staff, along with the instructional technology specialist in the School of Education. The instructional technology specialist in Academic Computing & End-User Support Services coordinates training workshops and provides instructional design support and consultation to the faculty. This position also works with the Virtual College staff to provide faculty training in the areas of course design and instructional support for the use of Blackboard, the university’s course management system. The instructional technology specialist assigned to the School of Education assists professors and pre/in-service teachers with incorporating technology into the teaching and learning experience. Training is also provided to non-teaching employees in the use of standard application software. A computer lab is designated as the training lab for faculty & staff.

Campus Teaching and Learning with Technology (CTLT) includes the support, equipment, and facilities needed to use information technology to enhance the educational process from course planning and content development through the pedagogical process and assessment:

ECSU Campus activities in support of this strategic focus are:

- Enhancing campus TLT activities through research and training workshops
- Engaging faculty and other users in TLT related conversations through roundtable/brown bag discussions.
- Assessing the effectiveness of TLT efforts through customer surveys
- Creating a collaborative TLT Program by engaging technology users from all academic disciplines and support areas.

**UNC IT Strategy Focus 2: Distance Education (e-learning)** is the educational process in which the majority of instruction occurs when student and teacher are not in the same place. Instruction may be synchronous or asynchronous and may employ correspondence study, audio, video or computer technologies.

The Virtual College extends availability and access to on campus courses via distance education to prospective students who are isolated from campus due to time and/or geographic location.

ECSU Campus activities in support of this strategic focus are:
1. To expand accessibility to on campus courses via e-Learning to those who are isolated from campus due to time and/or geographic location. Utilization of existing, new, and emerging technologies will be incorporated.
   - Promote e-learning courses throughout the twenty-one county region and other selected areas.
   - Showcase the Virtual College at ECSU’s Technology Expo annually.
   - List Elizabeth City State University online courses with the Southern Regional Electronic Campus web site.

2. To supply faculty with available resources essential to develop, refine and deliver online courses.
   - Integrate technology into course delivery methods through training faculty to use an online course management system (Blackboard). The course management system will allow instructors to deliver course content to their students in traditional face-to-face courses and courses taught totally online.
   - Train additional full-time faculty to use the course management system (Blackboard).
   - Train additional adjunct and evening/weekend faculty to use the course management system (Blackboard).
   - Train faculty members to incorporate multimedia into their online and web-enhanced courses by learning to utilize the Tegrity Web Learner Studio equipment cart. Implemented Summer 2002.
   - Web-enhance additional courses taught at ECSU by using web-based technologies to increase access to course information. All courses will have a web presence for student access using the Blackboard course management system.

3. To positively impact enrollment and increase student retention.
   - Expand e-learning course offerings to reflect all academic majors currently offered on campus.

4. Work towards preparing an academic department to offer at least 50% of a degree online.
   - The Virtual College will be targeting the Business and Economics Department to design, develop and deliver 50% of their business administration degree online.
   - The Virtual College is also working with the School of Education and Psychology to design, develop and deliver a percentage the core teacher licensure courses online.

**UNC IT Strategy Focus 3: Services for Students** encompasses the administrative processes that students experience throughout their educational lifecycle from pre-enrollment through graduation and alumni relations.

ECSU IT activities in this area are:

- Implemented Web-enabled Services for Students which allows
  1. Students to pre-register and register for classes
2. Review catalog for course descriptions and degree requirements, check course schedules
3. Review their transcripts and review grades immediately after grades are posted by faculty
4. Review financial status of account (money owed, financial aid awarded)
   • Implemented Wireless Network Access in the Residence Halls
     ▪ Students have access to campus network and the Internet
   • Manage and support personal computer labs for student use
   • Implementing Campus Pipeline – Portal for Student Services. Alumni /Development System (ADS) Installed for use by Alumni and Development Offices

**UNC IT Strategic Focus 4: Administrative Systems** includes the processes of system procurement, implementation, operations and maintenance, user support and training, and data sharing for the financial, human resource, student information, and alumni/development systems.

ECSU IT activities in this area are:

- Participating as a full member of the Shared Services Alliance, additional applications and user training have been provided
- Working through and with the Alliance, the Office of the President negotiated and contracted with vendor for the applications and training, resulting in improved services and support to the user community at an affordable cost
- Working through the Alliance, ECSU is planning to migrate all administrative applications from SIS/Plus to Banner
- With the migration to Banner, the university will have access to a relational database, which will provide the capability for data sharing as needed across the user community.

**UNC IT Strategic Focus 5: Logistical Needs** is defined as the infrastructure, support services, processes, training and other factors needed to achieved the objectives of the other four issue areas.

ECSU IT activities in this area are:

- Network and application security capability installed and operational
- All classroom and administrative buildings have been wired consistent with UNC IT Minimum Wiring Standard
- All residence halls have been wired for wireless capability in the rooms--port by every pillow. One residence hall has both wireless and wiring consistent with the UNC IT Minimum Wiring Standard. As existing residence halls are renovated, they will be upgraded to have CAT-5e wiring as well as wireless connectivity.
• New residence halls will have both CAT-5 as well as wireless this includes the current privatized housing project.
• All buildings have access to the campus fiber backbone network
• Network access at the desktop can be either 10 or 100 Megabits
• Enhanced User Support and Training is available
• Collaborative Procurement Program is available through the Shared Services Alliances
• Process and procedures are being redefined as part of the Banner migration effort

Reference(s):


Support of the Board of Governors Strategic Directions

The UNC Board of Governors Information Technology Strategy is outlined in the “University of North Carolina Board of Governors: Long Range Plan 2002-2007”. ECSU’s support of this strategy is contained in the “ECSU Strategic Plan: 2002-2007”. The Transformation and Change section of this document gives an overview of the IT efforts that are planned and implemented for supporting the UNC Board of Governor’s IT Strategy. Also the support is the same as documented under the five UNC IT Strategic Focus areas. The five UNC IT Focus areas are listed as follows:

• Teaching and Learning with Technology
• Distance Education (e-Learning)
• Administrative Systems
• Services for Students
• Logistical Needs

Reference(s):


ECSU Strategic Plan: 2002-2007
Organization

IT Functional Responsibilities

The Division of Information Technology provides centralized IT service for the University. It is divided into three groups, two of which are led by a Director, and the Chief Information Officer is the acting Director of the third group. The IT management staff at ECSU has IT management experience in both the private sector and IT management experience in higher education. The CIO has 38 years of experience in Information Technology. Of the 30 years of private sector experience 25 years were spent in IT management. All eight years of higher education experience have been in IT management. The director of Administrative Computing has 35 years of experience in the Information Technology field. Thirty years were spent in the private sector and the other 5 in Higher Education. The director of Academic Computing has 13 years of experience in Information Technology. All 13 years have been spent in Higher Education. The following is an overview of the responsibilities of the groups that report to the CIO:

**Administrative Computer Center (Information Systems)**, which is responsible for maintaining a solid base of technically, oriented computer-related support for the entire university. Its mission include serving as a viable data processing agency for the university, managing efficiently the administrative computing resources of the university, supporting the development of the management information system, and providing the means for its users to meet their goals and objectives. These services include the administrative functions using SCT's applications such as the Financial Records System (FRS), the Student Information System (SIS), the Financial Aid Management (FAM), the Human Resources System (HRS), the Alumni Development System (ADS), and Fixed Assets. The work of the department includes the following:

- To program, test and document the functional users required modifications to the existing applications.
- To serve as the primary consultants to functional users regarding technical utilization of the various application systems.
- To serve as the first level support for problems related to the application systems.

**Academic Computing & End-User Support Services**, which provides a broad range of assistance to administrators, faculty, staff, and students. This support includes instructional technology, computer lab support, web design and hosting, employee training in the use of productivity software. The department provides end-user support services for all areas of the University. These services include pre-purchase consultations, hardware/software configurations, instructional design, technical troubleshooting & problem resolution, email, web services, and network server support. This department is directly responsible for the four computer labs and the faculty/staff training lab in the Information Technology Center.
Network Services & Telecommunications, which provides voice and data support. The campus data and voice network infrastructure are increasingly central and critical to the University mission and day-to-day operations. Also, the data and voice networks are becoming increasingly integrated, supporting the traditional data applications, video and telephone/telecommunications services as well as laptop wireless networks. Telecommunications develops the requirements and specifications for campus upgrades and negotiates with vendors and contractors for the implementation of the innovative networks. Additionally, telecommunications operates the systems for controlling access to the campus network and administrative systems, allocation of network resources and bandwidth available to users and applications. Telecommunications is also responsible for the campus Wide Area Network connections including access to the Internet as well as the NCREN connections and applications.

IT Organization Charts
Standing IT Committees

The Information Technology Planning and Policy Council (ITPPC) is the only standing IT committee on campus. At times subcommittees are appointed by the chairman of the ITPPC to address specific topics. Based on needed expertise and topics being addressed, individual are picked to serve on subcommittees that are not members of the ITPPC. The chair of the subcommittee will be a member of the ITPPC.

This Council develops university-wide policies and procedures associated with all aspects of Information Technology systems and processes. These policies and/or procedures address telecommunications (voice, video and network services), electronic data processing, acquisitions and deployment of IT resources, and the appropriate use of campus IT resources. The council serves in an advisory role in the strategic planning for IT at the university. Updates and recommendations are given at least quarterly to the Administrative Council based upon monitoring campus IT operations and external IT developments.

Composition of ITPPC:

Chief Information Officer, Chair
Vice Chancellor for Business and Finance
Director of Administrative Computing
Director of Academic Computing
Director of Library
Director of Virtual College (e-learning)
Instructional Technology –Teacher Education
Instructional Technology - General
Registrar
2 Faculty Members (Selected by Faculty Senate)
2 Staff Members (Selected by Staff Senate)
1 Student (SGA President or selected by SGA)

IT Decision Making Process

The CIO is the focal point for all IT decisions on campus. The CIO reviews and approves the purchase/acquisition of all computer related hardware and software. The review ensures compliance with strategic directions, need and compliance with state purchasing guidelines. Based on the impacts that a product implementation will have on the entire university, the CIO will seek approval from the Chancellor, the ITPPC and the Administrative Council. The CIO reviews decisions that have been made by the Shared Services Alliance Board of Directors so that the university is supportive of these decisions. User community support is key to having a successful IT plan.
IT Infrastructure, Policies, Procedures and Standards

Policy Approval Process

Information Technology policies are developed by a subcommittee of the Information Technology Planning and Policy Council (ITPPC). Once the policy is developed, it is reviewed and approved by the ITPPC. The policy is then sent to the Administrative Council membership for review and comments. Once the comments have been received and addressed by the ITPPC subcommittee it is then reviewed and approved again by the full ITPPC. The policy will now be sent to the Administrative Council where a vote will be taken at the next scheduled meeting of this Council. Once approved by the Administrative Council, the Chancellor makes the determination if the policy is one that should be reviewed and approved by the Board of Trustees before implementation takes place. A policy can go into effective after being approved by the Administrative Council or after approval by the university’s Board of Trustees is received.

Project Planning Process

The CIO and his staff are members of the Advisory Committee, which convenes monthly.

UNC CAUSE Meetings:

UNC CAUSE was established in 1970 by the sixteen University of North Carolina campuses for the purpose of promoting cooperation and information exchange between the campuses of the UNC System in all areas related to information technology. (Reference: www.uncause.org)
Elizabeth City State University takes an active part in the annual UNC CAUSE Fall Conference by sharing and collaborating on best practices through delivering and attending formal presentations and birds-of-a-feather meetings, as well as participating in informal networking.

IT Infrastructure – Campus Backbone and Network Description

Elizabeth City State University recently enhanced its campus infrastructure by implementing a Cisco based network to interconnect the campus. This switched network provides the bandwidth, the flexibility, and the capability of growth to support all foreseeable University networking demands over the next five years. This network includes a 4-node LAN Core switching concept with Gigabit connections to stackable distribution switches located in each campus building. These are fiber links, which allows a backup path for each of the core switches. All port speeds will support either 10 or 100 Mbps data transport speeds to the desktop. The campus network is wired consistent with the University of North Carolina IT Phase 1 Strategy wiring standards. Additionally, all of the Residence Halls currently have wireless internet access capability, and as the dormitories are renovated, all will eventually have dual internet access capability, wireless as well as physical cabling.

Security:

The network includes a redundant Internet Firewall with a single Demilitarized Zone (DMZ). The management is configured on a separate server. Internet Intrusion Detection (IDS) is also provided on a separate server. Additionally, the network includes a redundant Intranet Firewall to protect the Administrative Computing Resources. The Data Center and Server Room have controlled and limited access.

The University’s critical applications require passwords for access. Modifications of the application software are protected from abuse by an electronic software control procedure. Information security is managed and controlled in accordance with the university’s Information Security Policy.

Additionally, all University desktop computers are password protected, and in areas controlling critical financial, personnel and student data, unattended systems are keyboard locked after five minutes.

IT Infrastructure – Administrative Applications

The following Systems and Computer Technology (SCT) applications are being used to meet the Administrative Computing needs at ECSU:
1. Financial Records System, including:
   a. Financial Accounting
   b. Accounts Payable
   c. Purchasing
   d. Fixed Assets
   e. Accrual
   f. On-Line Requisitioning

2. Student Information System, including:
   a. On Course (Degree Audit)
   b. Housing Module
   c. EDI.Smart
   d. On Line Registration
   e. Student Transcript viewing and updating

3. SIS Financial Aid Module, including:
   a. Packaging Aid Resource

4. Human Resources System

5. Alumni Development System

6. E-Print

7. FOCUS for Reporting

Computer Room Services and Hardware

Data Center

The Data Center is an 880 square feet computer room housing a Clustered DS20E Compaq Duel Alpha servers) running an OpenVMS Operating System (7.2-1). The peripheral devices include two high-speed printers, a Compaq Storageworks TL891DLX Mini-library, (Disk Drive). The Data Center provides administrative and academic computing services for the entire campus. These services include the administrative functions using SCT’s applications such as the Financial Records System (FRS), the Student Information System (SIS), the Human Resources System (HRS) and the Alumni Development System (ADS). The Data Center also houses the Web for Students and Web for Faculty applications that provide a variety of academic functions. Additionally, the Data Center houses the Mainsaver server and the Payment Gateway system that provides the capability of payment by credit card.

The Data Center has controlled and limited access, a controlled environment, a raised floor, a sprinkler system and a Mitsubishi 2033A Series UPS system.

Server Room

The university has maximized support & service through the strategic relocation of servers from across campus locations to an 1180 square feet server room. In this location the Network Administrator manages and supports servers supporting various academic and administrative
operations including e-mail, web, virus protection, calendaring, DHCP, e-learning, administrative support, Student Health Services, Luminus, ID/POS, and Financial Aid.

The Server Room has a sprinkler system and a Mitsubishi 2033A UPS system.

Help Desk and Student Help Desk

A formal Help Desk is not offered at this time. However, Administrative Computing and Academic Computing provide computing services and assistance to faculty, staff and students. These services include telephone support for IT related problems such as desktop computing support, student computing issues (labs and wireless communications), PC repair and maintenance, security and virus protection as well as telephone support.

Student Computer Labs

There are four open labs in the Information Technology Center available to students and faculty. These labs are available for general purpose computing activities as well as for instructional use. In addition to these labs, there are approximately 22 other computer labs located in academic departments on the campus, which in most cases support discipline specific research and applications.

Library Systems

The Library is wired and workstations are available for use by library patrons. In addition to the Card Catalogue System, patrons have access to a variety of on line databases. Faculty, staff and students can access the card catalogue system from any workstation on campus.

University Web Page

The University web page is designed to provide relevant and timely information to students (prospective and current), faculty, staff, alumni, and friends of the university. At the time of this report, a new design, which will be ADA compliant, is being implemented.

Wireless Connectivity

All of the residence halls and the Information Technology Center at ECSU have wireless connectivity to the Internet and the campus network. One residence hall has both wireless and CAT-5E wiring. Over the next 12 to 18 months, wireless connectivity will be expanded to classrooms and other selected common areas on campus.
Management Processes

The CIO is the focal point for all IT management decision at ECSU. The Information Technology Planning and Policy Council has the responsibility for establishing, reviewing and approving all University Wide IT policies and procedures.

The need for a university wide IT policy may originate from anyone on campus. The CIO will appoint a sub committee from the ITPPC membership to research the need and then draft this policy if research supports the need for such a policy.

The policy is then circulated to the entire council for review and comments. Once comments have been received and factored into the draft, the policy is reviewed and approved at the next monthly ITPPC meeting.

Once this Council has approved the policy they policy is then sent to the Administrative Council membership for review and comments. Any suggested changes are given to the sub committee for either incorporating into the policy or rejecting the suggestion.

The updated policy is then sent to the ITPPC for final approval prior to the policy being submitted to the Administrative Council for a formal approval. The approval of the Administrative Council is required prior to a policy going into effect.

Some policies are taken before the Board of trustees for review and approval before they are put into effect. The decision to have a BOT review is made by the Chancellor in conjunction with the CIO.

The last step in the policy approval process is to put the policy on the web. A similar path is used for major campus wide procedures. Procedures are not taking beyond the Administrative Council for approval.

Acquisitions for Major IT Goods and Services

The acquisition of all IT goods and services require the approval of the CIO. State purchasing guidelines are used for the acquisition of IT goods and services. Any single purchase that exceeds ECSU’s purchasing limit of $35,000 is reviewed and approved by State purchasing. If an item is not on the State contract and the cost exceeds $2,500 the item is bid with three bids being required. Sole source justification is used only when a single vendor provides the goods or services being requested.

Major IT Implementation Projects

The university uses buy product solutions as opposed to developing new products. This approach is more cost effective for us. Our implementation cycle is installing, testing and doing some customization of off-the-shelf products. As part of the acquisition of the product we also
contract with the provider, when needed, to assist us with the installation, customization, testing and training. As a full member of the Shared Services Alliance we have been able to enhance and extend our IT goods and services that are being provided by the small IT staff at ECSU through collaboration. Our process is as follows:

**Project Implementation Process Flow**

1. **Problem**
2. **Evaluate**
3. **Acquire**
4. **Install**
5. **Customize**
6. **Test/Validate**
7. **Train**
8. **Production**
9. **Support**
10. **On Demand**
IT Life Cycle Management

The University has adopted a “PC Replacement Policy,” which governs the acquisition and disposal of personal computers. The life cycle of personal computers is three years. In some instances the life cycle may extend to four years. If a computer no longer meets the needs of an employee, but it could be used to satisfy a current need elsewhere on campus, the computer is returned to the Information Technology Center to be reformatted and re-issued to another user. Once it is determined that the computer cannot be used to satisfy a need at the university, the equipment is transferred to Fixed Assets for disposal.

Network infrastructure equipment is replaced as needed, based on the growth of campus requirements and General Administration Network guidelines.

IT Professional Development And Training

Due to the availability of funds, professional development is limited. Staff members do get an opportunity to attend UNC Cause. They also have the opportunity to attend other key user group conferences. On campus workshops and seminars are used for training and knowledge transfer for selected topics. When a new applications, systems and new technologies are implemented at the university, training and knowledge transfer takes place are part of the implementation. The required training and skills is provided by the by the product vendor. At other times it is provided by the outside agency that assist with the installation. We have used train the trainer as well as training the required technical staff and key users.

Disaster Recovery and Business Continuity Planning

In addition to the procedures described in the Disaster Recovery Plan, the university has methods for manually registering students and paying bills.

Customer Requests & Complaints

The CIO and department directors monitor customers’ requests and assign the task to be completed to the appropriate personnel. The IT management team also receives complaints via email, phone calls, and face-to-face contact with customers. Complaints are noted, shared with employees, and resolved when possible.

State EDP and Financial Audits

The last formal IT audit was conducted by the State Auditor’s office from September 26, 2000 through November 9, 2000. The primary purpose of the audit was to evaluate the IS general controls that were in place during that time frame. The results of that audit are documented in the following document entitled:
Conclusion

Elizabeth City State University has a robust IT infrastructure that includes a central IT organization that provides a full range of computing services to the university community. A value-added amenity to the IT unit at ECSU is the Information Technology Center which houses all major IT functions under a single roof—the Office of the CIO, Administrative Computing, Academic Computing, Telecommunications & Network Services, NC-REN, and the Virtual College. This facility affords one-stop shopping for end-user support and services.

The IT planning process is driven by a committee structure. Major IT decisions and initiatives are well informed by the various constituents at the university. The ITPPC is comprised of a representative and diverse group of employees and students. When it is necessary, appropriate subcommittees are formed to further inform the decision-making process.

The university has a formal approval process for managing IT purchases, developing and implementing IT initiatives. Implementing the PC Replacement Policy has enhanced this process.

Elizabeth City State University systematically monitors its strategic planning process, ensuring a dynamic and structured instrument for guiding and evaluating the progress of the university. ECSU’s strategic plan, the IT strategy, the UNC system’s Strategic Plan, and the UNC system’s IT Strategic Plan share the appropriate links which yield practical as well as accountable IT decisions at ECSU.

It should be clear to the readers of this document that Elizabeth City State University has the necessary management staff and internal controls to prudently plan, acquire, implement, and deliver information technology. The SAC’s review process and the excellent report of the IS/IT
audit attest to the university’s ability to discharge its responsibilities with integrity, civility, and sensitivity.
I. Introduction

The Elizabeth City State University (hereinafter “University”) computing and telecommunications networks, computing equipment and computing resources are owned by the University and are provided primarily to support the academic and administrative functions of the University. The use of this equipment and technologies is governed by federal and state law, and University policies and procedures. Additional rules and regulations may be adopted by various divisions/departments to meet specific administrative or academic needs. Any adopted requirements must be in compliance with applicable federal and state laws, and this policy.

II. Regulatory Limitations

A. The University may monitor access to the equipment and networking structures and systems for the following purposes:

   1. To insure the security and operating performance of its systems and networks.
   2. To enforce University policies.

B. The University reserves the right to limit access when federal or state laws or University policies are violated or where University contractual obligations or University operations may be impeded.

C. The University may authorize confidential passwords or other secure entry identification; however, students have no expectation of privacy in the material sent or received by them over the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above.
D. The University generally does not monitor or restrict material residing on University computers housed within a private domicile or on non-University computers, whether or not such computers are attached or able to connect to campus networks.

E. All material prepared and utilized for work purposes and posted to or sent over University computing and other telecommunications equipment, systems or networks must be accurate and must correctly identify the creator and receiver of such.

F. Any creation of a personal home page or a personal collection of electronic material that is accessible to others must include a disclaimer that reads as follows:

The material located at this site is not endorsed, sponsored or provided by or on behalf of the University.

III. Permissible Use

Students are expected to follow this policy and any related University rules, regulations and procedures for University work produced on computing equipment, systems and networks. Students may access these technologies for personal uses if the following restrictions are followed:

A. The use is lawful under federal or state law.

B. The use is not prohibited by Board of Governors, University or institutional policies.

C. The use does not overload the University computing equipment or systems, or otherwise harm or negatively impact the system’s performance.

D. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).

E. The use does not violate federal or state laws or University policies on copyright or trademark.

F. The use does not state or imply University sponsorship or endorsement.

G. The use does not violate state or federal laws or University policies against race or sex discrimination, including sexual harassment.

H. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.
IV. Suspension of Privileges by System Administrator

A. The University's System Administrator may suspend a student's access privileges for as long as necessary in order to protect the University's computing resources. As soon as practicable following the suspension, the System Administrator must take the following actions:

1. The student must be provided with notice of the suspension and the reasons for it.
2. The student must be given an opportunity to meet with the System Administrator to discuss the suspension if the student requests it.
3. Following the meeting, the student must be notified that the student may appeal to the System Administrator's immediate supervisor if the student is dissatisfied with the outcome of the meeting.

B. If the System Administrator believes that this policy has been violated, the System Administrator may refer the matter to [the appropriate disciplinary mechanism].

V. VIOLATION OF POLICY

A. Any violation of this policy is "misconduct" under the University's student conduct code. Violations should be reported as provided in that code.
B. Sanctions for violation of this policy may include revocation or suspension of access privileges in addition to any other sanction permitted under the student conduct code.
C. Violations of law may also be referred for criminal or civil prosecution.
ELIZABETH CITY STATE UNIVERSITY
Internet Acceptable Use Policy

Preamble

The Internet is an electronic highway connecting computers all over the world, making it possible for millions of people to share and/or exchange information. Internet access is coordinated through a collaborative effort of government agencies, and regional and state networks. The Internet offers vast, diverse, and unique resources to students, faculty, staff, and administrators. Such services include electronic mail and graphical access to the World Wide Web. This policy governs the use of Internet resources at Elizabeth City State University.

1. Acceptable Use

Elizabeth City State University’s primary goals in providing Internet services to the university community are to support research and education, and to enhance institutional effectiveness and efficiency. The use of university resources must be in support of these goals.

2. Inappropriate Use

Transmission of any material in violation of any national, state, or university regulation is prohibited. Except where it is explicitly permitted, it is a violation of one or more university policies, state or federal law(s) for users of the university's Internet resources to:

   A. Provide copyrighted material without copyright permission.
   B. Provide obscene, defamatory, or harassing language or material, or use the resources to defame or harass.
   C. Provide material for personal commercial gain.
   D. Provide commercial services.
   E. Receive compensation, from any party not entitled to utilize university resources for production or distribution of material.
   F. Provide materials whose nature or volume compromises the ability of the resources to serve other users (e.g., chain mail).
   G. Use network resources to view or transmit pornography or other objectionable material.
   H. Make a malicious attempt to harm or destroy data of another user.
   I. Download copyrighted material (e.g., music) without written permission or proper payment if it is of a commercial nature.

3. Violation of Policy

_The use of the Internet is a privilege, not a right._ Sanctions for violation of this policy may include revocation or suspension of access privileges in addition to any other sanction permitted under university code. Violations of law may also be referred for criminal or civil prosecution. Refer to ECSU’s _Computer Use Policy_ for other regulatory information.
5. Application of Public Records Law

All information created or received for work purposes and contained in university computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records Law applies. This information may be purged or destroyed only in accordance with the ECSU records retention schedule and State Division of Archives regulations.

6. Review

ECSU reserves the right and has the authority to interpret and apply this policy and the Board of Trustees has the authority to review and/or modify or amend it at any time. It is imperative that each employee reviews and complies with any changes made to this policy.
ELIZABETH CITY STATE UNIVERSITY  
Laptop Loan Policy  

Preamble  

Elizabeth City State University (ECSU) has reserved a limited inventory of laptop computers at the Circulation Desk of G. R. Little Library for loan to students. This policy shall govern the usage of the laptop computers on loan at G. R. Little Library.  

1. Eligibility  
Currently enrolled ECSU students with valid student identification cards, valid G. R. Little Library accounts and who sign laptop loan agreements are the only individuals eligible to borrow laptop computers from the Circulation Desk at G. R. Little Library. ECSU reserves the right to refuse to loan a laptop computer to any student who has damaged an ECSU laptop computer or who violates this policy.  

2. Ownership  
   A. All laptop computers made available for loan at G. R. Little Library are and shall remain the property of ECSU.  
   B. ECSU reserves the right to terminate the loan of a laptop computer, without advance notice, if it appears that a laptop has been abandoned or used in violation of this policy.  
   C. There shall be no expectation of privacy with regard to any information stored on any loaned laptop computer. ECSU reserves the right to review any and all information contained within the laptop computer at any time without advance notice to the borrower.  

3. Loan Periods and Availability  
   A. Laptops may be checked-out from the Circulation Desk of G. R. Little Library during the library’s hours of operation until two (2) hours before the library closes but may not be reserved in advance.  
   B. Laptop computers may be checked out for a maximum period of three (3) hours. The loan period may be renewed for an additional 3-hour period, if availability allows.  

4. Restrictions on Use  
   A. In-Library Use Only: Laptop computers will be issued to students on loan for use exclusively within G. R. Little Library.  
   B. Physical Possession: Students shall be required to keep laptop computers issued on loan in their physical possession at all times until returned to the Circulation
Desk. Incidents involving loaned laptop computers being removed from G. R. Little Library shall be reported to Campus Police.

C. **Tampering Prohibited**: Students are prohibited from: tampering with the hardware or software of loaned laptop computers; attaching hardware or loading software on loaned laptop computers.

D. **Educational/Research Use Only**: Loaned laptop computers shall be used exclusively for educational purposes relating to class assignments and research.

5. **Late Fees and Liability**
   A. **1st Hour Overdue**: A late fee in the amount of five dollars ($5.00) shall be assessed if a loaned laptop computer is returned late.
   
   B. **More than an Hour Overdue**: A late fee in the amount of ten dollars per hour ($10.00/hr.) shall be assessed if a loaned laptop computer is more than one hour overdue.
   
   C. **24 Hours Overdue**: Any laptop computer that is more than twenty-four hours overdue shall be reported to Campus Police.
   
   D. **Damage/Loss/Theft**: Students shall be financially responsible for paying the costs of any damage, loss or theft that may occur to a loaned laptop computer up to a maximum of $1,100 plus any applicable late fees. If a loaned laptop computer is stolen while under a student’s possession, late fees shall cease to accrue when the student reports the theft.
   
   E. **Collection**: ECSU shall use student billing to collect any late fees or amounts assessed for laptop computer damage or replacement costs.

6. **Violations**
   Violations of this policy shall result in immediate suspension of privileges to borrow laptop computers reserved at G. R. Little Library and may result in other disciplinary action.
1. **Preamble**

Elizabeth City State University (ECSU) has established this plan to comply with the federal law on safeguarding customer financial information. In accordance with the Gramm-Leach-Bailey Act ([http://banking.senate.gov/conf/grmleach.htm](http://banking.senate.gov/conf/grmleach.htm)), ECSU has developed certain administrative, technical or physical safeguards pertaining to accessing, collecting, distributing, processing, protecting, storing, using transmitting, disposing of or otherwise handling customer information, as defined in Section VII.A below. The safeguards collectively constitute the university’s information security program.

2. **Information Security Plan Coordinator**

The Director of Network Services is designated as the coordinator for ECSU’s information security program.

The coordinator shall assist the university community in identifying reasonable, foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

3. **Risk Assessment and Safeguards**

As part of the risk assessment, the coordinator shall work with all segments of the university community to identify possible or existing risks to security and privacy of customer information. Division heads shall be responsible for conducting periodic data security reviews under the Coordinator’s guidance.

The coordinator, as part of the risk assessment, shall determine possible or existing risks with the university’s information systems, including network and software design, as well as information processing, storage, transmission and disposal.

The coordinator, as part of the risk assessment, shall make reasonable efforts to detect, prevent and respond to attacks, intrusions or other system failures.

The coordinator, as part of the risk assessment, shall design and implement information safeguards to control risks identified through risk assessment and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.
4. Employee Training and Education

Training and education sessions will be developed (by whom) for all university employees who have access to covered data including but not limited to: (1) employees within the Information and Technology Department who have general access to university data; (2) employees who are custodians of covered data and (3) employees who utilize covered data in carrying out job responsibilities.

5. Oversight of Service Providers and Contracts

ECSU shall take reasonable efforts to select Service Providers, as defined in Section 7.B. below, who implement and maintain the required safeguards for customer information. The Office of Business and Finance, in consultation with the Assistant to the Chancellor for Legal Affairs, shall make written requests of all Service Providers to provide assurances of compliance with the GLB Act.

All contracts entered into prior to June 24, 2002 shall be grandfathered until May 24, 2004.


This plan shall be subject to an annual review to ensure continued compliance with applicable laws and regulations.

7. Definitions

A. Customer information refers to any record containing nonpublic personal information as defined by 16 CFR 313.3(n)(1)\(^1\) whether in paper, electronic, or other form than is handled or maintained by or on behalf of ECSU.

B. Service Provider refers to any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to ECSU.

\(^1\) 16 CFR Part 313.3(n)(1) defines nonpublic personal information as “personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publically available.” An example includes information that a student provides on the Free Application for Federal Student Aid (FAFSA).
Preamble

Elizabeth City State University (ECSU) is committed to providing the university community with a secure network environment. This policy is designed to protect the integrity and insure the stability of the network operated by ECSU Office of Information Technology (the campus network) from fraudulent use and/or abuse resulting from access and use of the network. This policy applies to all individuals who utilize ECSU’s computing and electronic communication resources including but not limited to: faculty, staff, students or other authorized users who are not otherwise affiliated with ECSU. Access by other authorized organizations or individuals outside the ECSU organization is determined on a case-by-case basis and is limited to the required action and the time frame necessary to complete the function that individual has come to accomplish.

1. Definitions

Under this policy, the following terms are defined accordingly:

A. Access Control: The management of admission to system and network resources. The first part of access control is authenticating the user, which proves the identity of the user or client machine attempting to log on. The second part is granting the authenticated user access to specific resources based on university policies and the permission level assigned to the user or user group.

B. Dynamic Host Configuration Protocol (DHCP). DHCP is a protocol by which a machine can obtain an IP address (and other network configuration information) from a server on the local network.

C. Domain Name System (DNS). The Domain Name System is the system that translates Internet domain names into IP addresses. A "DNS Server" is a server that performs this kind of translation.

D. Fire Wall: A combination of hardware and software that separates a network into two or more parts for security purposes.

E. File Transfer Protocol (FTP). FTP is a way to login to another Internet site for the purposes of retrieving and/or sending files.

F. Encryption: A process involving data coding to achieve confidentiality, anonymity, time stamping, and other security objectives.

G. Enterprise: University-wide.

H. Local Area Network (LAN). A computer network (or data communications network), which is confined in a limited geographical area.

I. Mission Critical Data: Data that is vital for the university to function harmoniously. The unavailability of such data would prevent the university from operating.

J. Server: Any computer that provides services to any other computer over a network e.g., Microsoft Internet Information Server, Apache HTTP Server, Telnet and FTP Servers, Norton PC Anywhere, Virtual Network Computing (VNC), Napster, Audio Galaxy Satellite, etc.
K. The Secure Shell (SSH) is used to protect UNIX systems and users. It creates an encrypted channel so the data is not visible as clear text.

2. Responsibility of Users

A. Responsibilities of All Users

   i. Overall Security of Systems All users of ECSU’s computer systems and network resources have the responsibility of ensuring the overall security of ECSU’s systems as set forth in this policy and other Information Technology (IT) policies, guidelines and/or procedures.

   ii. Compliance with Applicable Policies All users are responsible for becoming knowledgeable and complying with this policy and other IT policies, guidelines and/or procedures.

B. Responsibilities of the Network Services Department

ECSU’s Network Services Department (NSD) has oversight for telecommunications and data services at ECSU. The NSD has the same user responsibilities as set forth in Section 3.A. above and the additional responsibilities and privileges listed below:

   i. The NSD shall assess the security of ECSU servers, workstations, network resources, and data, and define and recommend best practices regarding security of data and systems.

   ii. The NSD shall conduct vulnerability scans on a regular basis to ensure the security of ECSU’s systems, network and data, and if necessary to recommend a course of action to mitigate any vulnerabilities.

   iii. The NSD shall recommend campus standards for security, and to routinely review relevant policies and procedures in the context of the standards for security.

   iv. The NSD shall investigate, evaluate and implement approved security related technologies, such as authentication/authorization mechanisms, encryption, certificate services, antiviral software, network monitors, and firewalls.

   v. The NSD shall provide assistance in the resolution of serious security compromises, including providing assistance for recovery and security. The NSD will collaborate with the university police department or other administrative divisions, as necessary.

   vi. The NSD shall work in conjunction with departments on campus to establish campus-wide standards for security and access control.

C. Responsibilities of System Administrators

System administrators have the same user responsibilities as set forth in section 3. A. above plus the additional responsibilities and privileges listed below:
i. System administrators shall act as local information systems security coordinators.

ii. System administrators shall establish appropriate user privileges, monitor access control logs, and perform similar security actions for the systems they administer.

iii. System administrators shall register (provide name and contact information) with the NSD and be adequately trained to provide network services for their network’s operating environment.

iv. Backup system administrators shall register (name and contact information) with the NSD and be adequately trained to provide network services for their network’s operating environment.

v. System administrators shall prepare and maintain security procedures in their local environment that implement the Network Security Policy.

vi. System administrators shall prepare and maintain access control, backup and disaster recovery plans in the event of a disaster.

vii. System administrators shall take reasonable precautions to safeguard against corruption, compromise or destruction of data, computer systems, and network resources.

viii. System administrators shall ensure that user information is treated as private. It is recognized that a system administrator may potentially have contact with user files, email, etc. in the course of his or her duties. The contents of such files must be kept private. Access to system user files is authorized only in the event of a security investigation and must be approved by the Chief Information Officer (CIO) or his/her designee.

ix. System administrators shall take reasonable and appropriate steps to see that all hardware and software license agreements are executed and maintained on all systems, LANs, and servers.

x. System administrators shall participate in security training and other activities provided by the NSD.

xi. System administrators shall participate on school or department initiated projects (committees) that may impact the information technology resources at ECSU.

3. General Administration

A. Each user will be made aware of the Network Security Policy and other IT policies, guidelines and/or procedures through employee training sessions, e-mails, departmental staff meetings, and the ECSU website.

B. Individuals aware of any breach of information system or network security, or compromise of computer security safeguards, shall report immediately such situations to the system administrator or the departmental representative responsible for security in that area. The system administrator must determine if a security breach has occurred, and if so, shall report the incident immediately to the Director of Network Services and/or the CIO.

C. System administrators shall acquire prior written approval from the NSD before making configuration changes or installing network devices, such as switches.
D. Faculty, staff or students shall not establish their own personal web servers, FTP servers, news servers, LANs to existing LANs, or other multi-user systems for communicating information without the specific approval of the NSD.

E. Enterprise services, such as Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), e-mail, routing, WINS services, firewalls, e-mail relay services, and directory services must be run in cooperation with the NSD.

F. Security protocols, such as SSH (Secure Shell) and SSL (Secure Sockets Layer) must be used whenever possible.

G. Port scanning within the ECSU’s LAN is prohibited without the explicit permission of the NSD.

H. Packet sniffing is strictly prohibited by personnel outside the NSD.

4. Physical Security

A. Non-mobile computing equipment must be placed in an environmentally controlled location (e.g., temperature, humidity, exposure to water, etc.).

B. Core computing resources and equipment must be stored in secure locations (server room, wiring closets, etc.) with restricted access.

C. Printers or faxes used for sensitive data must be stored in a secure location.

D. Magnetic media such as hard drives, diskettes, flash drives, zip drives, tapes, or other electronic storage media must be erased before disposal or transfer.

E. A crosscut shredder must be used for the disposal of sensitive documents.

F. Uninterruptible Power Supplies (UPS) are required for networking devices and servers.

G. Where appropriate, security access and authorization documentation must be retained a minimum of three (3) years.

H. IT administrators shall have access to information technology to maintain systems in the event of a compromise or potential security issues.

I. Mission critical data, or a copy of it, must not be stored on a laptop or a handheld device.

J. Vendors, consultants, contractors, and their affiliates shall not be left unattended in core network locations.

5. System Security

A. Only authorized personnel shall install applications on a server or workstation.

B. The local system administrators shall determine administrative access to servers. Administrative access shall only be given to authorized personnel whose primary daily tasks require administrative access.

C. System configuration must be done off line. The system must not be connected to the network until it is at an appropriate level of security.

D. Whenever system security has been compromised, or even if there is a convincing reason to believe that it has been compromised, the involved system administrator shall immediately (within the same hour of discovery): (a) reassign all relevant passwords, and (b) force every password on the involved system to be changed at the time of the next log-in. If the compromised system’s software does not provide the
latter capability, the system administrator shall send a broadcast message to all users instructing them to change their passwords.

E. All devices attached to the network must be attached to a managed domain or network.

F. Operating systems and applications must be kept current. Where appropriate, all the latest operating and application patches must be applied.

G. Applications must be configured securely.

H. Security, account, and system level logging must be turned on when a server is initially set up.

I. The use of fault tolerant systems, such as disk mirroring, server duplexing, or RAID is recommended. This is required for servers that store mission or business critical data.

J. Major applications must be installed on dedicated servers, e.g., mail on its own server, Web files on a separate server, etc.

K. Maintenance and Service Agreements with vendors must be kept current.

6. User Account Security

A. Only authorized personnel shall install applications on a server or workstation.

B. Each user shall have a unique user ID. System administrators must be able to uniquely identify all users, including name, user ID, association, phone number and location.

C. The “Administrator” passwords to mission critical systems must be recorded and saved in a secure location for emergency reference.

D. Each user’s profile must not be readable, writeable or executable by other users. Access to shared resources should be granted only as needed.

E. Accounts created for vendors to provide services must only be active during the time the service is being performed.

F. Accounts must be re-certified annually to ensure that only valid accounts remain active.

G. All user accounts, where possible, must automatically have the associated privileges revoked after a 90 days of inactivity.

H. Temporary accounts must be assigned expiration dates at the time of creation.

I. If possible, failed login sessions must be terminated and the account locked after five (5) unsuccessful attempts.

J. Where possible, concurrent logins under a unique user ID must be limited to one (1).

7. User Access for Separated Employees, Transferred Employees and Employees on Leave Status

A. Notice of Change in Employee Status: The Division of Human Resources and payroll shall report all changes of employment status to the Director of Network Services on the effective date of change.

B. User Access:
8. **Password Administration**

A. All accounts must have assigned passwords.
B. Administrators and support staff shall never request users to reveal their passwords. If an administrator must sign on to a user’s account, the password must be reset to give access to the administrator for support services. The user shall be required to change his/her password after the administrator completes the support service.
C. Network administrators and other support staff shall be prohibited from disclosing users’ ID and passwords to anyone.
D. Users shall be required (through software authentication) to change their passwords after initial login to a server.
E. Password history, where possible, must be activated and the last six to ten passwords kept.
F. Minimum password length must be eight (8) characters, including special characters and numerals.
G. Maximum password age, where possible, must be between forty and fifty days.
H. Passwords must not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, or in other locations where unauthorized persons might discover them.
I. Passwords must not be written and left in a place where unauthorized persons might discover them.
J. All passwords must be changed immediately if they are suspected of being disclosed, or known to have been disclosed to anyone besides the authorized user.
K. The system administrator must change all vendor-supplied default passwords before any computer or communications system is used.
L. Password files must be encrypted.
M. Additional password standards in the Minimum Password Complexity Standards must be followed.

9. **Communications**

A. Encryption should be used when a high degree of confidentiality is required for email communication.
B. Communication software and dialing in through modems attached to a workstation must not be used. ECSU provides a Virtual Private Network (VPN) appliance to connect to ECSU’s intranet.

10. Wireless Devices

A. Wired Equivalency Protocol (WEP) will not be mandatory on access points.
B. Sensitive applications must not be hosted on wireless subnets or be transmitted over the wireless network.
C. No systems on wireless subnets shall store or transmit data of a sensitive nature such as credit card numbers; private student information, legal or attorney privileged data.
D. All users of wireless subnets shall acknowledge these policies and agree to abide by them before access is granted to wireless subnets.
E. The NSD shall administer all wireless access points.
F. The CIO or his/her designee shall approve any exceptions to the above.

11. Computer Viruses

A. To ensure continued uninterrupted service for both computers and networks, all desktop systems (personal computers) and servers must be configured for automatic anti-virus software updates. (UNIX systems are excluded at this time.)
B. All external media (e.g., flash drives, diskettes, etc.) should be scanned before using them on desktops and servers.

12. Backups

A. System administrators or backup administrators shall make sure that backups are completed, monitored and verified. Systems should be restorable after a failure, due to loss of data or a compromise, within a short period of time.
B. Backups must be stored in a secure environment not in the same room as the system.
C. Backups of critical systems must be stored in a secure environment offsite.
D. The number of sets and frequency of backups of a system must be based on the risk analysis of the system, application, or data being backed up.
E. Backup and restore procedures must be documented.
F. System administrators or backup administrators must test media periodically to determine its effectiveness.

13. Disaster Recovery

A. Each school or department must have a Business Analysis/Risk Assessment plan.
B. Each school or department must have a business continuity plan.
C. An inventory of hardware, software, service agreements, vendor contacts, personnel information and responsibilities must be maintained.
D. Business continuity plans must be reviewed and updated annually.
14. Compliance with Law and Policy

State laws prohibit theft or abuse of computers and other electronic resources. The following activities are specifically prohibited under this policy:

A. Interfering with, tampering with, or disrupting resources.
B. Intentionally transmitting any computer viruses, worms, or other malicious software;
C. Attempting to access, accessing, or exploiting resources you are not authorized to access.
D. Knowingly enabling inappropriate levels of access or exploitation of resources by others.
E. Downloading sensitive or confidential electronic information/data to computers that are not adequately configured to protect it from unauthorized access.
F. Disclosing any electronic information/data you do not have a right to disclose.

Violators of this policy may be denied access to the campus network. In addition to any possible legal sanctions, violators of this policy may also be subject to disciplinary action up to and including dismissal or expulsion, pursuant to ECSU campus policies, codes of conduct, or other instruments governing the individual’s relationship with ECSU. Recourse to such actions shall be as provided under the provisions of those instruments.
Elizabeth City State University
Banner Security Policy

Preamble
Elizabeth City State University (ECSU) is committed to taking all reasonable measures to ensure that its data is securely maintained. ECSU is utilizing Banner as its administrative computing tool or data repository to manage all administrative data such as student data, financial aid data, personnel data, etc. This policy shall govern the process for accessing and utilizing the Banner system and is applicable to all employees, students, service providers or other authorized users with access to data maintained in Banner.

1. Definitions

Under this policy, the following terms are defined accordingly:

A. **Banner Managers**: A committee comprised of Banner module (functional areas, e.g., Student, Finance, Financial Aid, etc.) owners, department managers and Information Technology (IT) personnel responsible for coordinating the development, implementation, maintenance, and general stewardship of the Banner information system at ECSU.

B. **Banner Module Administrators**: The individuals responsible for the administrative oversight of a given Banner module and ultimately responsible for the data within said system.

C. **Banner Security Team**: A committee comprised of Banner module owners and the Banner Security Coordinator responsible for determining and granting functional user screen access.

D. **Banner Steering Committee**: A committee of senior administrators who will provide a high-level review of planning, development, and implementation activities of the cross-functionality of individual SCT Banner modules. This committee also advises and prioritizes personnel resources that may be needed during the various phases of implementation and make appropriate policy decisions when needed.

E. **Data Trustee**: Data trustees are senior University officials (or their designees) who have planning and policy-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management for the good of the entire University. Individuals participating on the Banner Steering Committee are Data Trustees or selected to represent their respective areas.

F. **Data Steward**: Data stewards are University officials having direct operational-level responsibility for information management – usually department directors. Data stewards are responsible for data access and policy implementation issues. Banner Managers and
Module Administrators consist of Data Stewards selected by their respective Data Trustees.

G. **Data Custodian:** The Information Technology Department, under the leadership of the CIO, is the data custodian. The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges to system users as authorized by data trustees or their designees (usually the data stewards), and implementing and administering controls over the information. The Chief Information Officer, IT Directors, the Banner Security Coordinator and other designated staff members of the Information Technology collectively functions as the Data Custodian.

H. **Data User:** Data users are individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.

2. **Data Ownership**

   A. Banner data is the property of ECSU. Access to Banner data is restricted to employees, students, and Service Providers authorized under this policy to have access. Access by any person(s) not authorized under this policy is strictly prohibited.

   B. Banner Module Owners have the sole authority to authorize access to the data within the modules they administer. Module Owners shall grant this access only at the level and to the extent necessary for the requestors to perform their job.

3. **Data Use**

   A. Banner data shall be used for official university business or as required by law. The use of Banner data for personal gain or curiosity, or another’s personal gain or curiosity, is prohibited.

   B. Persons and processes accessing Banner data will uphold the confidentiality and privacy of individuals whose data they access; and observe any laws, regulatory requirements, policies and ethical restrictions that may apply with respect to their accessing, using or disclosing such information.

   C. Persons and processes with access to Banner data, regardless of its form (electronic or print), will ensure that reasonable measures are taken to protect the data from theft, unauthorized or accidental viewing, copying, downloading, modification and/or destruction. The Banner Security Coordinator in the Department of Administrative Computing is to be notified immediately in the event the security of any Banner or other administrative data is compromised.
D. Persons with access to Banner data shall direct individuals with a formal request for information, subpoena or court order to the University’s Legal Affairs Office using appropriate channels.

E. Anyone in the service of ECSU, with a genuine business or educational need, may be authorized to access the Banner data necessary to perform his/her duties by the appropriate data steward as determined by the data trustee. An individual's access to Banner data will be discontinued when the individual leaves the service of the university or during an extended leave of absence. Supervisors are to notify the Director of Administrative Computing and the Office of Human Resources immediately when an employee is separated from employment or begins an extended absence.

4. Data Safeguards

A. Banner data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk.

B. Security measures for data are set by the data custodian, working in cooperation with the data stewards.

5. Reporting Violations

Any suspected violations of this policy, or unauthorized access to computing resources, or any other condition which could compromise the security of Banner data or other university computing resources must immediately be reported to the Department of Administrative Computing Security Coordinator.

6. Sanctions for Non-compliance

Violators of this policy may be denied access to the campus network and subject to disciplinary actions.

7. Enforcement

Enforcement measures, such as periodic reviews of access assignments, requirements and inspections of audit controls, implemented for data security will be dictated by the data-classification level, which is on a need to know basis. Measures will include an appropriate combination of the following:

A. Audit controls

B. Change control and process review

C. Data protection and access control
D. Data-retention requirements
E. Documented backup and recovery procedures
F. Data disposal
G. Encryption requirements
H. Storage locations
I. User awareness
ELIZABETH CITY STATE UNIVERSITY
Data Classification Policy

Preamble

Data stored here at Elizabeth City State University is a critical asset. All employees of the University community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (such as in electronic, paper or other physical form). Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of data belonging to the University to be in compliance consist with state and federal law.

This policy serves as a foundation for the University’s information security policies, and is consistent with the University’s data management and records management standards. The University recognizes that the value of its data resources lies in their appropriate and widespread use. It is not the purpose of this policy to create unnecessary restrictions to data access or use for those individuals who use the data in support of University business or academic pursuits.

1. Scope

This policy applies to all centrally managed University enterprise-level administrative data and to all user-developed data sets and systems that may access these data, regardless of the environment where the data reside (including mainframe systems, servers, personal computers, mini-computers, etc.). The policy applies regardless of the media on which data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

2. Policy

Data must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with data value, sensitivity, and risk.

A. To implement security at the appropriate level, establish guidelines for legal/regulatory compliance, and reduce or eliminate conflicting standards and controls over data, data will be classified into one of the following categories:

i. Restricted – data whose disclosure to unauthorized persons would be a violation of federal or state laws or University contracts Examples include student or employee identifiable information. (i.e., Social Security Number, birth date, driver’s license number, etc.), financial records, medical records, legal records, student records, police records, and credit
card information. Unauthorized disclosure of restricted information could result in adverse legal, financial or reputational impact upon the University).

ii. **Public** – data to which the general public may be granted access in accordance with the North Carolina Public Records Act. (Examples include public web pages, course listings, press releases, marketing brochures, etc. While the requirements for protection of public data are less than that of Restricted and Sensitive, sufficient controls must be maintained to protect unauthorized modification of data).

iii. **Sensitive** – sensitive data is information that business units may decide to share with other units outside their administrative control for the purpose of collaboration. This information is not information that meets the requirements of “non-public” information. (Examples include data created by the department, research data, and project data. Loss of this information could cause harm to the University’s image or reputation, but would not necessarily violate existing laws or regulations).

Data in all categories will require varying security measures appropriate to the degree to which the loss or corruption of the data would impair the business or research functions of the University, result in financial loss, or violate law, policy or University contracts.

B. Security measures for data are set by the data custodian, working in cooperation with the data stewards, as defined below.

The following roles and responsibilities are established for carrying out data policy:

i. **Data Trustee**: Data trustees are senior University officials (or their designees) who have planning and policy-level responsibility for data within their functional areas and management responsibilities for defined segments of institutional data. Responsibilities include assigning data stewards, participating in establishing policies, and promoting data resource management for the good of the entire University.

ii. **Data Steward**: Data stewards are University officials having direct operational-level responsibility for information management – usually department directors. Data stewards are responsible for data access and policy implementation issues.

iii. **Data Custodian**: Information Technology is the data custodian. The custodian is responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, backup
and recovery processes, granting access privileges to system users as authorized by data trustees or their designees (usually the data stewards), and implementing and administering controls over the information.

iv. **Data User:** Data users are individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.

Clarification of roles in data classification is the responsibility of Administrative Computing department of the Information Technology Division.

3. **Enforcement**

Enforcement measures implemented for data security will be dictated by the data-classification level. Measures will include an appropriate combination of the following:

A. Banner Security Policy  
B. Acceptable Use of Technology for University Employees  
C. Network Security Policy

4. **Review**

The Director of Administrative Computing will review the policy periodically and bring concerns to the Chief Information Officer, which will recommend revisions as appropriate.
ELIZABETH CITY STATE UNIVERSITY
Information Security Incident Response Policy

Preamble

This policy outlines the procedures for decision-making regarding emergency actions taken for the protection of Elizabeth City State University (ECSU) information resources from accidental or intentional unauthorized access, disclosure or damage.

1. Applicability

This policy is applicable to all University students, faculty and staff and to all others granted use of Elizabeth City State University information resources who become aware of an information security incident concerning a Network, Academic or Administrative Computing System. Every user of any of ECSU’s information resources has responsibility toward the protection of the University’s information assets; certain offices and individuals have very specific responsibilities.

2. Purpose

ECSU recognizes the need to follow established procedures to address situations that may indicate that the security of the University’s information assets may have been compromised. The purpose of information security incident response is to mitigate the effects caused by such an incident and to protect the information resources of the University from future unauthorized access, use or damage. Such procedures include ensuring that the appropriate level of University management becomes involved in the determination of actions implemented in response to an information technology security incident.

A standard University wide approach to information security events is important because of the following factors:

A. The need to promptly and effectively address any improper access of University information systems or the data they contain
B. Legal and regulatory requirements regarding the safeguarding of University information assets
C. The University’s implementation and reliance on University-wide applications, like Banner and Oracle, which impact the entire campus
D. Intellectual capital that ECSU both produces and owns needs to be protected against premature disclosure or unauthorized tampering
E. Damage to the University’s SACS accreditation status can have both direct and indirect negative effects
F. A general worldwide increase in the number and severity of computer security incidents
G. The need to protect the privacy of persons whose information is stored on information systems owned by the University
3. **Definitions**

**A. Information Security Incident** — An information security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of incidents include activities such as:

I. Attempts (either failed or successful) to gain unauthorized access to a system or its data
II. Unscheduled system down time or service interruption
III. Unwanted disruption or denial of service
IV. The unauthorized use of a system for the processing or storage of data
V. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

**B. Administrative Computing System** — Any application, or information system, that directly or indirectly deals with or supports financial, administrative, or other information that is an integral part of running the business of the University

**C. Academic Computing System** — Any application, or information system, that directly or indirectly deals with or supports the University’s primary mission of teaching, learning and research.

**D. Resources – Hardware, firmware, or software**

4. **Notification**

A member of the University community who becomes aware of an information security incident involving an Academic or Administrative Computing System must immediately:

A. Submit a security ticket to helpdesk@mail.ecsu.edu or directly to the IT Security Incidence Response Team at itsirt@mail.ecsu.edu or
B. Contact the University’s Administrative Computing Office that handles Information Security at 252-335-3319 or itsecurity@mail.ecsu.edu.
C. Upon recommendation of the Chief Information Officer, the University’s IT Security Incident Response Team may convene a fact-finding working group comprised of cognizant business and technical personnel and, where appropriate (such as instances where legal requirements are implicated, e.g., where private data of individuals is compromised), consult with the University Attorney, and communicate the incident to the Internal Auditor and the Vice Chancellor for Business and Finance or designate(s).
5. **IT Security Incident Response Team**

When warranted by information obtained during preliminary fact-finding, the University’s Information Security Officer will promptly convene a meeting with the Information Technology Security Incident Response Team (ITSIRT). Depending on the circumstances of each situation, the Information Security Officer shall include in the ITSIRT representation of some or all of the office/department affected in resolving the incident.

6. **Escalation of Decision-Making**

The ITSIRT will plan and coordinate the activities of all the offices involved, keeping other concerned offices advised as appropriate. In carrying out this responsibility, the ITSIRT will ensure that important operational decisions are elevated to the appropriate Vice Chancellor to protect the fundamental interests of the University and others impacted by the incident. Such decisions include, but are not limited to:

A. Restricting information system access or operations to protect against unauthorized information disclosures
B. Reporting and/or publicizing unauthorized information disclosures, as required by law
C. Involving law enforcement agencies in cases where applicable statutes appear to have been violated
D. The Information Security Office will also be responsible for documenting the deliberations and decisions of the ITSIRT as well as all actions taken pursuant to ITSIRT deliberations.

7. **Report Preparation**

The Information Technology Security Incident Response Team, jointly with the Internal Audit office, will be responsible for writing a final report(s) to the appropriate University office(s) which summarizes findings regarding the information security incident and, if appropriate, makes recommendations for improvement of related information security practices and controls.

**COGNIZANT OFFICE** — Information Technology, Information Security, Administrative Computing department, Internal Auditor, Network Services Department

8. **Information Technology Security Incident Response Team**

Consist of Information Technology staff responsible for the daily security of the University Administrative and Academic Systems.

**Members include:**
Director of Administrative Computing, Information Security
Director of Network Services, Network Security
Director of IT Client Services
Banner Security Coordinator
Internal Auditor
Network Engineer
Network Analyst
Network Analyst, Email Administrator
Datacenter Coordinator and Backup Administrator
Database Administrator
Administrative Computing, Secretary