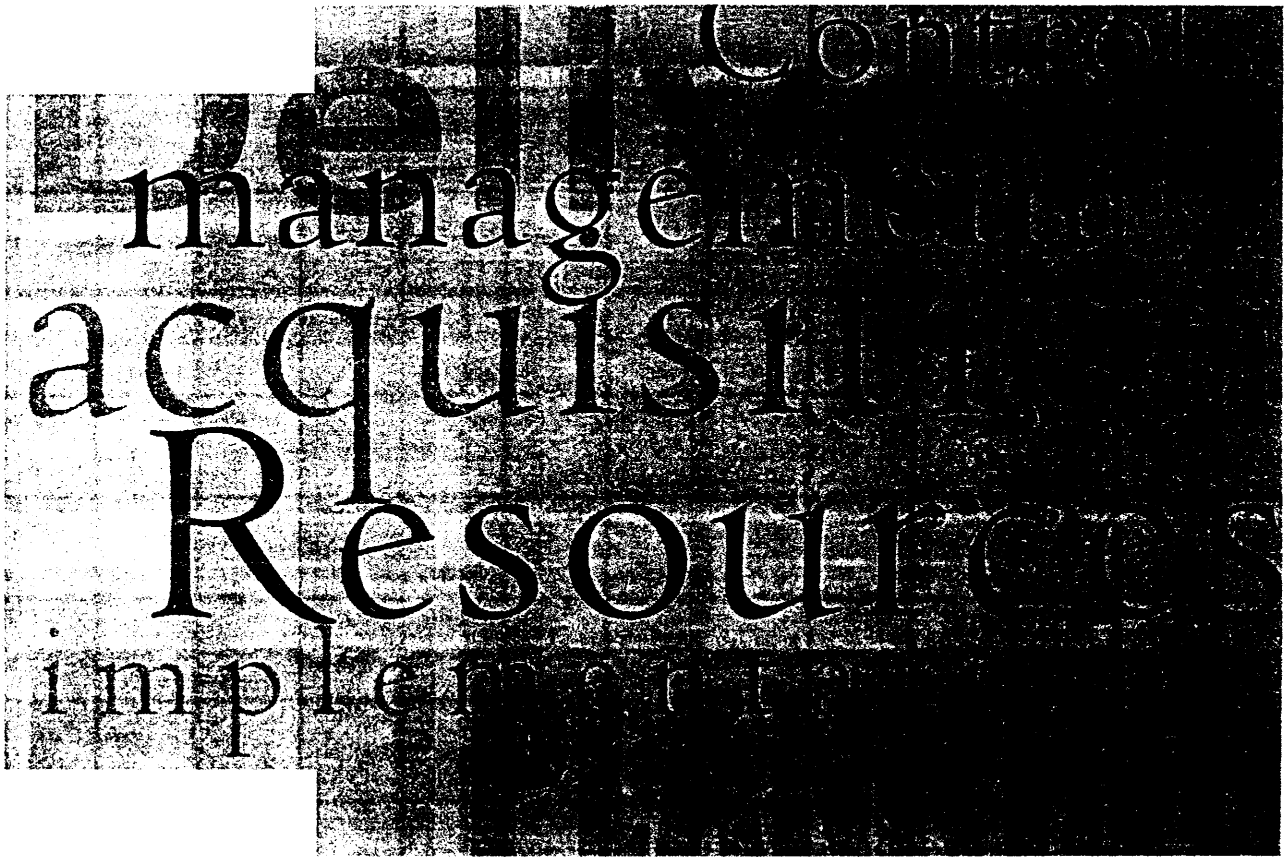
APPENDIX R

East Carolina University

Information Technology Management Flexibility Plan



Office of the CIO
East Carolina University
124 Austin Building
Greenville, NC 27858

October 4, 2002

Table of Contents

EXECUTIVE SUMMARY **1**

INTRODUCTION **3**

STRATEGIC PLANNING PROCESS **4**

CAMPUS STRATEGIC PLAN 5
UNC IT ROADMAP 5
BOARD OF GOVERNORS LONG RANGE PLAN 6
SUPPORT OF CAMPUS, UNC, AND BOG STRATEGIES 7

BOARD OF TRUSTEES RESPONSIBILITIES **9**

CENTRAL IT MANAGEMENT **10**

IT DECISION MAKING PROCESS **15**

POLICY APPROVAL PROCESS 15

IT INFRASTRUCTURE, STANDARDS, AND POLICIES **17**

IT INFRASTRUCTURE 17
CAMPUS IT POLICIES 17
University Policies *17*
ITCS Policies *17*
TECHNICAL STANDARDS 18
EDP Audit *18*
Disaster Recovery Plan (DRP)/Business Continuity Plan (BCP) *18*
ITCS Programming Standards Manual *18*
Service Level Agreements *18*
Student Computer Recommendations *18*
Supported Software and Hardware *19*

MANAGEMENT PROCESSES **20**

INFORMATION SYSTEMS/IT AUDIT PERFORMANCE 20
ACQUISITIONS OF MAJOR IT GOODS AND SERVICES 20
MAJOR IT PROJECT IMPLEMENTATION 22
IT LIFE CYCLE MANAGEMENT 22
IT PROFESSIONAL DEVELOPMENT AND TRAINING 22
DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING 23

ASSESSMENT AND ACCOUNTABILITY **25**

CUSTOMER SATISFACTION SURVEYS 25
STATE EDP AUDITS 25
ASSESSMENT RECORD BOOK 25
SACS REAFFIRMATION 26

FUNDING **27**

CONCLUSION **28**

BIBLIOGRAPHY **29**

APPENDIX A – UNIVERSITY IT POLICIES **30**

ACADEMIC COMPUTER USE POLICY 30
ACCOUNT TERMINATION POLICY 33
ADVERTISING POLICY 34
ANTIVIRUS POLICY 35
DEPARTMENTAL SERVER SUPPORT POLICY 38
DISK SANITIZING POLICY FOR WORKSTATIONS 40
ECU NETWORK USE POLICY 42
ECU NT DOMAIN PASSWORD EXPIRATION POLICY 43
EMAIL PURGE POLICY 44
NETWORK SCANNING POLICY 45
OPEN MAIL RELAY POLICY 48
SPAM E-MAIL POLICY 50
UNIVERSITY STUDENT AND EMPLOYEE COMPUTER USE POLICY 53
WORLD WIDE WEB POLICY 59

APPENDIX B - LIST OF INTERNAL ITCS POLICIES **61**

APPENDIX C - IT INFRASTRUCTURE **63**

IT INFRASTRUCTURE – GENERAL SUPPORT 63
Campus Backbone and Network Description *63*
Computer Room Services and Hardware *63*
Help Desk and Student Help Desk *64*
Student Computer Labs *65*
Internet Connection to NCREN *65*
Academic Library Services *65*
William E. Laupus Health Sciences Library *65*
OneStop Portal *66*
University Web Page *67*
Wireless Connectivity *67*
IT INFRASTRUCTURE – ADMINISTRATIVE SUPPORT 67
Administrative Applications *67*
Financial Data Warehouse *69*
IT INFRASTRUCTURE – FACULTY SUPPORT 70
Faculty Workstation Program *70*
Faculty Instructional Support – Academic Affairs IT Consultants *70*
Blackboard Services *71*
BSOM Student Computing Requirement For Laptops and PDAs *71*
University Multimedia Center *71*
Opscan Grading *72*
IT INFRASTRUCTURE – RESEARCH SUPPORT 72
CIITR (RAVE Laboratory) *72*
Research Support (Healthcare Data Warehouse) *73*
IT INFRASTRUCTURE – HEALTHCARE CLINICAL SUPPORT 74

IDX *74*
Logician *75*
Citrix *75*
Consolidation of Brody School of Medicine Informatics and CIS *76*
APPENDIX D – SDLC FORM 77

Executive Summary

East Carolina University requests the designation of special responsibility constituent institution under G.S. 116.30.1, so that the University is authorized to exercise management flexibility in the planning, acquisition, implementation, and delivery of information technology.

East Carolina University has the staff, resources, and internal controls required to competently administer and manage information technology (IT) on campus. East Carolina University demonstrates this capability by its:

- Support of the University of North Carolina IT Strategy and the Board of Governors' (BOG) Strategic Directions through a formal planning process
- Compliance with the University of North Carolina (UNC) baseline networking standards
- Excellent results in responding to electronic data processing (EDP) audits and resolving audit findings promptly
- Early production deployment of voice-over-IP (VoIP) telephony, wireless networking, remote access encryption, and web portal technology
- Solid organizational structure for the support and advancement of IT in education
- Processes and procedures for the selection, design, acquisition, implementation, and maintenance of IT
- Policies and standards for the responsible stewardship and improvement of IT
- Continuous assessment of IT activities by a dedicated internal IT auditor
- Funding provided by healthcare services, state appropriations, and grants.

East Carolina University's IT management, staffing, standards, and safeguards are organized into the following categories:

Centralized IT Management: ECU has a formal committee structure for the communication, collaboration, and input to campus IT projects and plans and a central IT support organization dedicated to data and telecommunications services, application development, system support, workstation and user support, data security, operations center services, and strategic initiatives.

IT Planning & Decision Making: ECU uses an established strategic planning process for the development of yearly information technology program plans to ensure that projects support the University's strategic objectives, the UNC IT Strategy and the BOG Strategic Directions. ECU also has a formal policy approval and project planning process that obtains campus-wide input to major IT decisions.

Infrastructure, Standards, and Policies: ECU has a highly-resilient, state-of-the-art fiber optic network operating at gigabit speeds with a high-speed connection to Internet and Internet2; administrative applications, such as financial, healthcare, and e-commerce; an Operations Center with approximately 200 systems housed in an environmentally controlled and physically secure facility; a help desk serving faculty, staff, and students via phone and online requests; wireless connectivity in selected classrooms, meeting rooms, and dining/public areas; and a web portal that provides students and faculty with a one stop online facility for accessing email, checking grades, registering for classes, and performing a variety of other important online activities.

Management Processes: ECU utilizes a proven process for purchasing IT goods and services, which results in better-informed purchasing decisions and reduced costs; uses a Systems Development Life Cycle (SDLC) for implementation of major IT projects; and has instituted an IT professional development program, known as the Staff Training and Education Program (STEP).

Assessment and Accountability: ECU undergoes EDP audits by the North Carolina Office of the State Auditor and the ECU Office of the Internal Auditor to identify strengths and weaknesses in IT systems and processes; utilizes assessment record books (ARBs) for the formal planning and evaluation of its administrative and educational support services; and performs a self assessment in conjunction with the Southern Association of Colleges and Schools (SACS) reaccredidation process.

Funding: ECU IT projects and services are funded through state appropriations, healthcare services, student computer technology fees, and grants. The University has specific processes for each funding source for the expenditure, review, and oversight of funding uses.

East Carolina University has the needed resources, controls, and management functions to competently exercise management flexibility in the planning, acquisition, implementation, and delivery of information technology.

Introduction

East Carolina University requests the designation of special responsibility constituent institution under G.S. 116.30.1, so that the University is authorized to exercise management flexibility in the planning, acquisition, implementation, and delivery of information technology. This report demonstrates that East Carolina University meets the requirements for management flexibility as set forth in Senate Bill 1005, Section 116-40.22.

This document provides a summary of ECU's IT planning, implementation, and oversight processes that adhere to industry standard practices. This document also shows how ECU's campus IT strategies are linked to the Board of Governor's Long Range Plan and the UNC IT Strategy to ensure consistency with the overall UNC goals. The Appendices provide the current University IT policies that govern the use and implementation of IT on campus and a description of the major elements of the campus IT infrastructure.

The information provided in this document demonstrates that ECU observes industry standard IT practices in its IT management processes with appropriate campus input and oversight.

Strategic Planning Process

East Carolina University's strategic plan, *Strategies for Distinction: University Directions, 2000–2005* [1], is the product of a formal development process, involving all departments, units, and administrative offices. Directed by the Advisory Committee on Strategic Planning, strategic and operational IT plans are developed, reviewed, assessed, and updated annually to ensure that they support the ECU strategic plan.

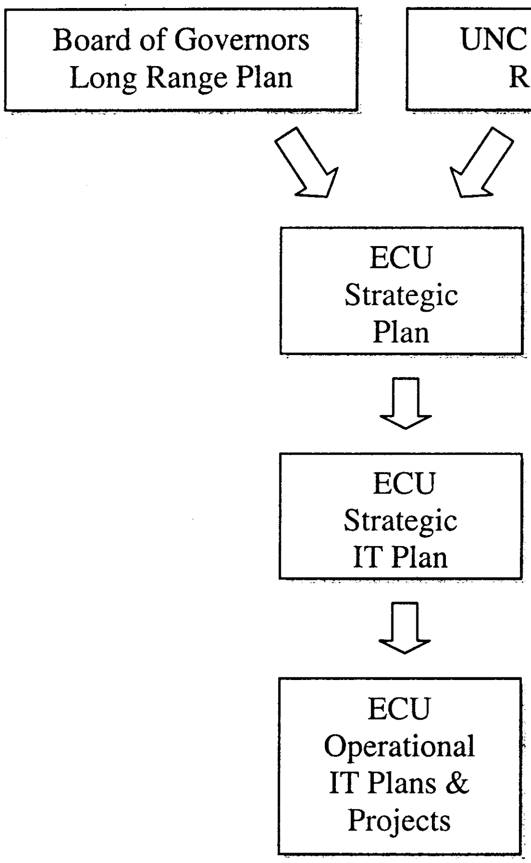

Board of Governors Long Range Plan
UNC IT Strategy Roadmap
ECU Strategic Plan
ECU Strategic IT Plan
ECU Operational IT Plans & Projects

Figure 1 – ECU Plan Development

As shown in Figure 1, the ECU strategic plan takes direction from the Board of Governors' *Long Range Plan 2002 – 2007* [2] and the University of North Carolina Office of the President's *A Roadmap to the Future* [3]. Additional information about the ECU strategic plan can be found on the ECU Planning and Institutional Research (PIR) web site [4].

The campus IT strategic plan, *ITCS Strategic Plan and Annual Report 2001-2002* [5], is a cross-cutting plan that supports all of the campus strategic planning goals and objectives as well the following University goal:

Goal 5: Be a leader in the development and application of information technology in higher education.

The campus IT strategic plan must be endorsed by the Information Resources Coordinating Council (IRCC) **[6]**. Implementation of the campus IT strategic plan requires a yearly IT Program Plan, which also must be approved by the IRCC. Projects specified in the program plan are implemented during the fiscal year and assessed at the end of the fiscal year. The accomplishments and project assessments for each fiscal year are contained in a "Year in Review" document that is available shortly after the end of the fiscal year.

Campus Strategic Plan

In the ECU campus strategic plan, the University defined strategic goals for the upcoming five-year period. The strategic goals associated with IT are as follows:

Goal 2-H: Strengthen opportunities for faculty to develop and apply innovative teaching strategies and for students to learn through new, innovative, and experiential settings.

Goal 4-C: Develop partnerships with health care, education, government, public service agencies, and industry for the coordination and application of information technologies to their needs.

Goal 5-B: Create a learning environment that fosters student appreciation and understanding of information technology as a lifelong learning tool.

Goal 5-D: Provide faculty, students, and staff with appropriate access to state-of-the-art services and technological infrastructure.

Goal 5-E: Enhance support services for high-performance computing, networking, and information technology.

Goal 5-G: Assist citizens, enterprises, and public agencies with easy and efficient access to the wealth of knowledge and data accessible at and through ECU.

UNC IT Roadmap

In 1999, the Board of Governors adopted the University of North Carolina's *Information Technology Strategy for the University of North Carolina: Advancing Campus Computing and Collaboration* **[7]**. This strategy is divided into five focus areas. These focus areas are as follows:

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

DE - ***Distance Education*** is the educational process in which the majority of the instruction occurs when student and instructor are not in the same place. Instruction may be synchronous or asynchronous and may employ correspondence study, audio, video, or computer technologies.

SS - ***Services for Students*** encompasses the administrative processes that students experience throughout their educational lifecycle from pre-enrollment through graduation and alumni relations.

AS - ***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.

LN - ***Logistical Needs*** is defined as the infrastructure, support services, processes, training, and other factors needed to achieve the objectives of the other four issue areas.

Board of Governors Long Range Plan

The UNC Board of Governors' Strategic Directions are explained by their long-range plan. The purpose of this Plan is to:

> *Delineate missions, establish major directions and strategies, and set strategic priorities for the University and its constituent institutions.*

The supported Board of Governors' Strategic Directions are as follows:

BOG Strategic Direction #2e. Strengthen undergraduates' knowledge and academic skill development to improve their chances of being successful in the workplace and in postgraduate studies.

BOG Strategic Direction #4a. Promote basic and applied research for the discovery and dissemination of new knowledge as a fundamental mission of the University.

BOG Strategic Direction #4b. Sustain UNC research, public service, and knowledge transfer activities that enrich the quality of life of North Carolina citizens through economic development, community outreach programs, and improved health, educational, and cultural resources.

BOG Strategic Direction #5d. Use technology to expand opportunities to exchange knowledge and ideas, and to make academic programs available across national boundaries.

BOG Strategic Direction #5h. Support research initiatives that expand UNC's ability to interact with international scholars on initiatives that are of state, national, and international interest and that benefit North Carolina and its citizens.

BOG Strategic Direction #6a. Expand campus Teaching and Learning with Technology (TLT) audiences beyond faculty to include librarians, instructional technologists, academic administrators, staff, and students; expand the portal to a professional development portal; and align TLT grants and workshop with e-learning strategies.

BOG Strategic Direction #6b. Implement coordinated technology platforms and services for e-learning both off-campus and in traditional classrooms. Develop and market existing UNC e-learning programs and courses. Develop policies and standards for coordinated offerings.

BOG Strategic Direction #6d: Complete remaining web-enabled student services and implement the Prospective Student Portal.

Support of Campus, UNC, and BOG Strategies

The Strategic Planning Matrix below summarizes the campus IT strategies and activities that support the ECU strategic plan, the UNC IT roadmap, and the BOG long-range plan. The campus IT strategies were developed as a part of the ITCS strategic planning process with the express purpose of providing direct support to the goals of the ECU strategic plan. The abbreviated designations for the different strategies are keyed to the descriptions in the preceding sections.

Campus IT Strategic Plan Strategies & Activities	Campus Strategic Plan	UNC IT Roadmap	BOG Long Range Plan
Campus IT Strategy #1: Advance the state-of-the-art in the application of technology to teaching and learning.	2-H	CTLT, DE	5d
Campus IT Strategy #2: Develop partnerships with regional health care providers, vendors and federal agencies to significantly enhance the health care services for the region.	4-C	AS	4b
Campus IT Strategy #3: Create training programs and enhancements to the curriculum to ensure that graduates will be well versed in the technologies in common use by potential	5-B	CTLT, LN	2e

employers.			
Campus IT Strategy #4: Provide state-of-the-art infrastructure for use by students, medical facilities, faculty, and staff by continuously updating student computing laboratories, the local and wide area network, classrooms, administrative computing, desktop hardware, desktop software, and collaboration capability.	5-D	CTLT, SS, LN	6b, 6e
Campus IT Strategy #5: Ensure that the skills and capabilities needed to establish and maintain ECU leadership in information technology are available by establishing programs to upgrade the skills of faculty and staff through employee development, training, and certification programs.	5-D	AS, LN	6a
Campus IT Strategy #6: Provide information technology expertise and facilities to enable faculty to conduct leading-edge research.	5-E	CTLT, LN	4a, 5h
Campus IT Strategy #7: Be an innovative leader in e-services to enable efficient, intuitive, convenient, timely, and secure access for student and administrative functions online from anywhere on the Internet.	5-G	DE, SS, AS	5d, 6a, 6b
Campus IT Activity #1: Establishment of the Center for Interdisciplinary Instructional Technology Research (CIITR) to be responsive to the goals of the UNC Teaching and Learning with Technology Collaborative.	2-H	CTLT	6a, 6b
Campus IT Activity #2: Establishment of the department of Distributed Education and Academic Information Technology (DEAIT) to coordinate the University's efforts in distance education.	2-H	DE, SS	5d, 6a, 6b
Campus IT Activity #3: Provide online course development and delivery software and services to the faculty.	5-D, 5-E	DE, LN, SS	6b
Campus IT Activity #4: Development of a university web portal that provides a secure, single point of contact for students, faculty, and staff for user-specific information, applications, and communications tools.	5-D, 5-G	SS, CTLT	6d

Board of Trustees Responsibilities

Senate Bill 1005, Section 116-40.22 specifies that the Board of Trustees shall establish policies and rules governing the planning, acquisition, implementation, and delivery of information technology and telecommunications at East Carolina University. The Board of Trustees shall submit all initial policies and rules adopted in areas specified in the legislation to the Office of Information Technology Services for review upon adoption by the Board of Trustees. Any subsequent changes to the policies and rules adopted by the Board of Trustees shall be submitted to the Office of Information Technology Services for review. Any comments by the Office of Information Technology Services shall be submitted to the Chancellor.

The Board of Trustees shall also report to the Board of Governors and to the Joint Legislative Education Oversight Committee any policies, procedures, and rules adopted in areas specified in the legislation prior to implementation. The report shall be submitted to both organizations at least 30 days before the next regularly scheduled meeting of the Board of Governors and shall become effective immediately following that same meeting unless otherwise provided for by the Board of Trustees. Any subsequent changes to the policies, procedures, or rules adopted by the Board of Trustees shall be reported to the Board of Governors and to the Joint Legislative Education Oversight Committee in the same manner.

The East Carolina University Board of Trustees is specifically responsible for approving University policies on information technology. By approving this plan, the Board of Trustees approves the existing University policies as listed in Appendix A.

The Board of Trustees specifically delegates the responsibility of approving new and modified ITCS internal IT policies and departmental IT policies to the Chancellor. The titles of the internal ITCS policies are listed in Appendix B.

The Chancellor shall submit annual information technology reports to the Board of Trustees for approval at the July meeting. The annual report will contain a summary of the IT accomplishments and changes in IT policies for the previous fiscal year.

Central IT Management

The Chief Information Officer (CIO) is responsible for creating the vision, plans, and implementation of campus-wide information technology initiatives. The central **Information Technology and Computing Services** (ITCS) unit that reports to the CIO carries out these initiatives. ITCS is organized into the following nine functional areas, each led by a Director.

Administrative Services handles all personnel actions, leave records, payrolls, budget management, travel, as well as providing administrative assistance to the CIO. This office is the central point of contact for questions that pertain to ITCS, both externally and internally.

IT Infrastructure provides a central contact point and coordination for the IT components of construction projects using both state bond funds and campus renovation funds. The Director of IT Infrastructure serves on campus construction and facilities committees and makes recommendations on IT issues to the CIO.

IT Consulting provides leadership, management, and support services to integrate computing technologies at East Carolina University. ITC is committed as a team to create an information technology infrastructure that facilitates access to information, problem resolution, and foresight in alignment with the academic missions and administrative functions of the campus.

IT Security manages the University's information technology security program. This program is broad in scope and covers security policy development, user awareness, user education, incident response and recovery, disaster recovery planning, implementation of the COBIT (Control Objectives for Information and Related Technology) standards, and user account security on the administrative mainframe. The mission of IT Security is to research, develop, and promote a secure digital environment that safeguards the University's electronic information and information technology.

IT Services supports the University's data network and telecommunications infrastructure. The mission of IT Services is to provide a high speed and robust communications networking environment to the University's end-users. This team is responsible for researching new technologies and discovering ways to implement them campus-wide.

IT Software Development Services is responsible for maintaining all existing and implementing new administrative systems and applications for the university. Major functional areas of support include: Business Services; Financial Systems; Student/Faculty Systems; Human Resources (including payroll); distributed applications/systems development; Patient Scheduling and Billing/Reimbursement; special projects for the Brody School of Medicine; university web development and portal applications; and centralized data base administration for all mission-critical systems.

Operations provides quality computer services and voice/data communication facilities for East Carolina University. The Operations section includes: an Operations Center for the main campus and the Brody School of Medicine, Production Control for both the main campus, and the Brody School of Medicine. Above all, ITCS Operations is a service organization with the main emphasis placed on providing quality service to the University's students, faculty, and administrators.

Project Relations provides support for the yearly program plans, the SACS assessment record books for ongoing evaluation of campus-wide IT projects, and external grant support. Project Relations created and supports the ITCS training and certification for IT staff across campus.

Strategic Initiatives promotes leadership in all areas of university information technology from a cross functional perspective and with an emphasis on the identification and development of grants and external funding opportunities, national IT initiatives, proposal writing, strategic university IT planning, and the aggressive exploration of the use of new and existing technologies in creative ways and in concert with University strategic goals.

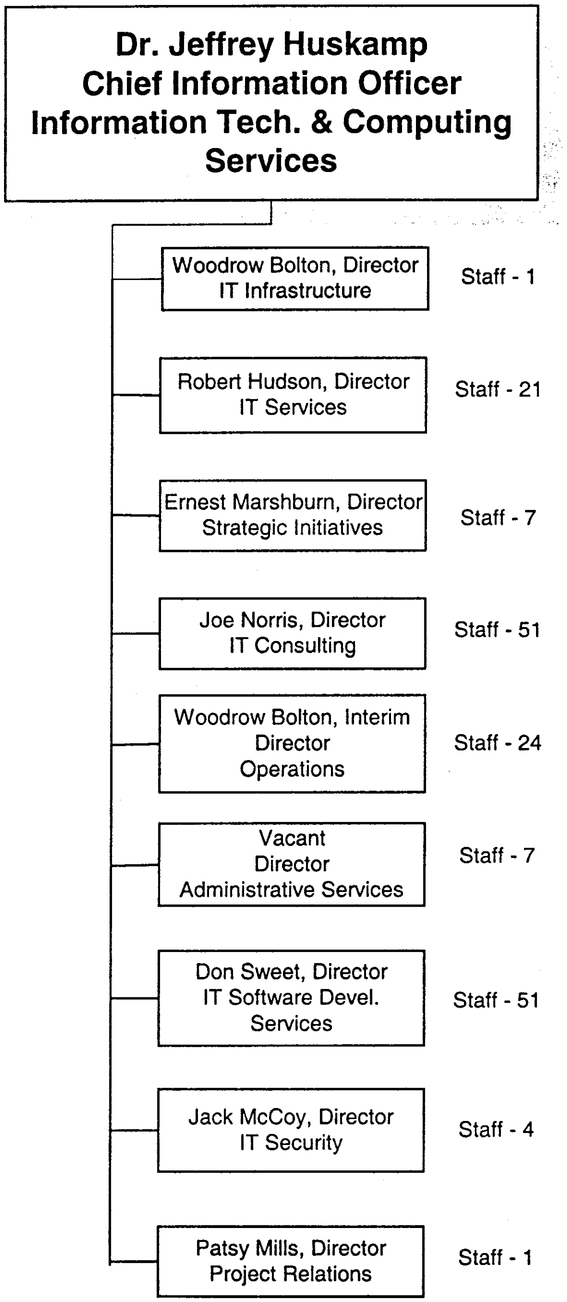


Figure 2 – Information Technology and Computing Services Organization Chart

The Chief Information Office receives advice from the **Information Resources Coordination Council** (IRCC) on campus information technology issues. The IRCC is composed of representatives from the major campus units and is a clearinghouse for IT information on campus. The Chief Information Officer chairs the IRCC to promote communication on information technology initiatives across campus. The charge of the IRCC is as follows:

> The Information Resources Coordinating Council (IRCC) makes recommendations to the Chief Information Officer on information technology coordination, collaboration, policy, and communication of actions by East Carolina University and its constituents. This includes but is not limited to recommendations on information technology planning, implementation, assessment, policies and other information technology related activities. The Council ensures communication between and makes recommendations on the actions of university committees, taskforces, administrative, and other bodies seeking to plan or implement information technology initiatives, including but not limited to IT policies, the planning and implementation of new projects, and the change or elimination of current projects or other actions. The routine work of the Council is carried out by its Executive Board.
>
> The Council shall review information technology policy, planning and implementation actions, and proposals to plan or implementations that may have a significant impact on the University. The Council receives from the Executive Board reports on its actions.

The IRCC has standing subcommittees to assist with specialized information technology areas and issues. These subcommittees are:

Academic Program, IT Policy and Academic Support Committee: This subcommittee is composed of nine members drawn from the faculty and the IRCC and reviews Academic Affairs and Health Sciences program plans involving IT. This subcommittee also reviews campus-wide IT policies before they are brought before the entire IRCC, reviews academic support policies and implementation, and coordinates distance education IT actions across campus.

Administrative Computing Committee (ACC): The ACC is composed of 13 members from academic, financial, business, human resources, information technology, and other administrative areas. The charge of this subcommittee is to design, implement, and maintain the most cost-effective methods to deliver functionally and technically, essential administrative services to meet the needs of customers in support of the academic, research, public service, and patient care missions of East Carolina University. This committee also approves and prioritizes major administrative technology initiatives for the campus.

Information Systems Steering Committee (ISSC): The Information Systems Steering Committee (ISSC) is composed of the major departments in the Brody School of Medicine and the Medical Foundation Practice Plan. The ISSC considers and approves information technology policies, procedures, and programs that are strategic for the Brody School of Medicine and its relationship to the Pitt County Memorial Hospital and other ECU units.

Student Computing Technology Fee Committee (SCTFC): The SCTFC is composed of eight members representing students, faculty, and IRCC members. The committee makes recommendations on the expenditure of funds obtained from the student computing technology fee receipts. These funds are the main support for student computing laboratories across campus and improvements to the student computing environment.

Vision, Strategy, and Planning Committee: This committee is composed of nine members representing faculty and IRCC members. The committee engages in university-wide information technology strategic planning, recommends prioritization of campus-wide initiatives, reports on the status of IT strategic planning goals, and makes recommendations on strategic IT infrastructure issues.

IT Decision Making Process

The decision making process at ECU utilizes a well-defined framework for development and requires university-wide collaboration. The following is from the *SACS Self-Study Committee Report, Section III. Institutional Effectiveness* **[8]**:

> Planning has been a formal, university-wide exercise since the late 1980s. Strategic planning provides a mechanism for communication throughout the university community; a platform for articulation of institutional goals; an organizational framework for making decisions, particularly those that allocate scarce resources among units with competing needs; and a vehicle for improving the effectiveness of the institution's programs, activities, and services.

The ECU strategic plan is used to focus and direct the information technology initiatives on campus. Before the beginning of a fiscal year, a program plan containing central IT campus-wide project descriptions, project budgets, and project assessments is created by ITCS. The Brody School of Medicine Executive Committee reviews the health sciences projects in the program plan. The CIO is notified which health sciences projects are funded before the beginning of the fiscal year. The IRCC provides advice to the CIO on the need and priority of the Academic Affairs projects. When the University budget for the fiscal year is finalized, the CIO, based on the IRCC input, determines which projects will be funded for the fiscal year. The CIO also looks for additional funding to implement projects not able to be funded from the base budget to provide as robust an infrastructure as possible.

Policy Approval Process

University IT policies may originate from any number of sources, but must take a designated path for university approval. The draft policy is first reviewed for adoption by the IRCC. Once recommended by the IRCC, the policy is transmitted to the CIO for approval. Once the CIO approves, the policy is presented to the Chancellor's Cabinet and then the Chancellor for review and approval. If the policy is a University-wide policy, the Chancellor submits the policy to the Board of Trustees for final approval. Once all the approvals are obtained, the policy is placed on the ECU web site and advertised as needed to ensure the ECU community is aware of the new policy. The approval process is shown in Figure 3.

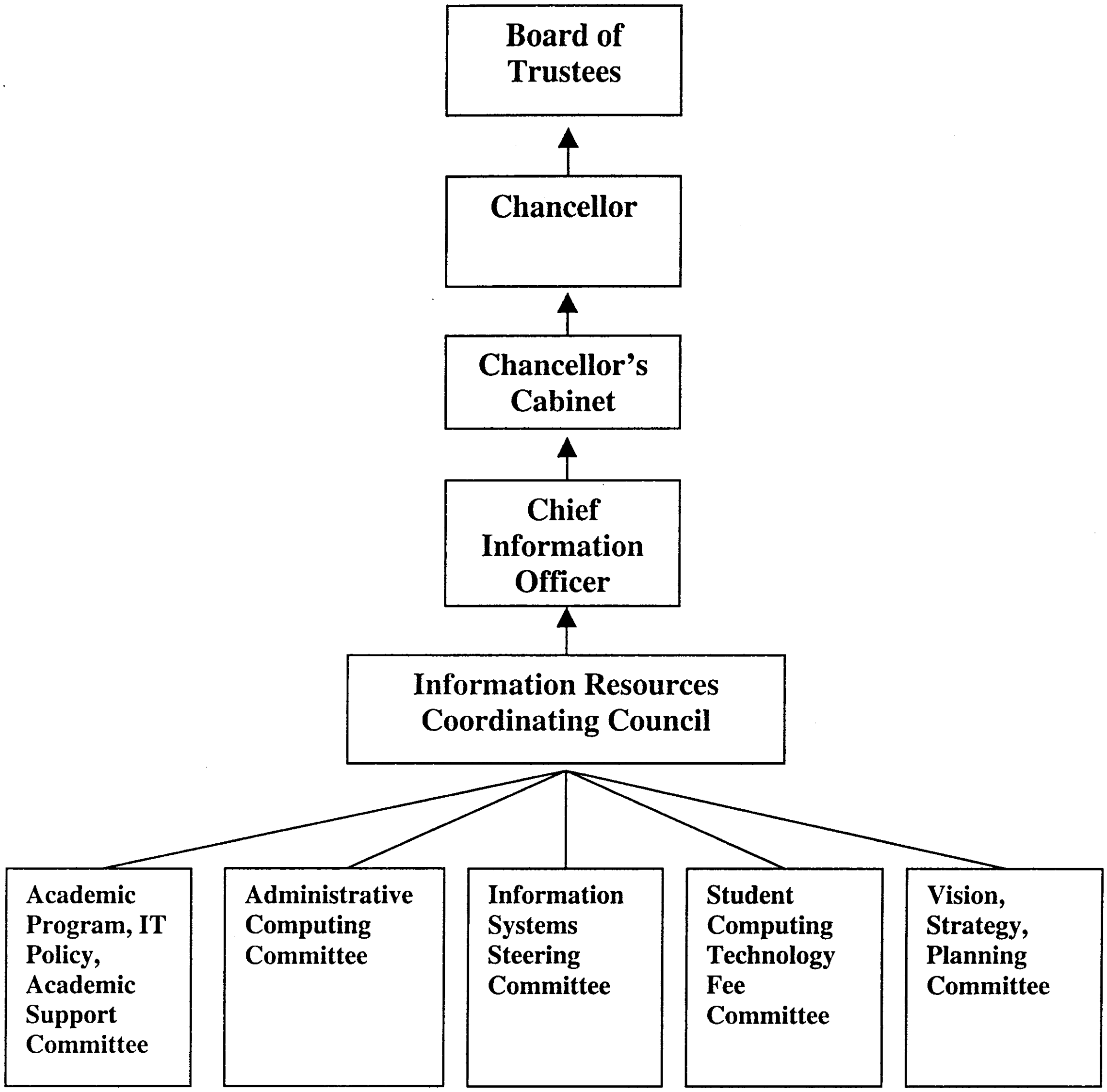

Board of Trustees
Chancellor
Chancellor's Cabinet
Chief Information Officer
Information Resources Coordinating Council
Academic Program, IT Policy, Academic Support Committee
Administrative Computing Committee
Information Systems Steering Committee
Student Computing Technology Fee Committee
Vision, Strategy, Planning Committee

Figure 3 – ECU Information Technology Approval Process

IT Infrastructure, Standards, and Policies

IT Infrastructure

East Carolina University has made significant investments in campus information technology infrastructure. ECU has been among the leaders in the university system in the following: deployment of wireless technology; providing workstations to faculty; increasing the campus bandwidth to the Internet; providing distance education course management systems; creating and developing a campus portal for faculty, staff, students, and prospective students; deploying voice-over-IP telephony technology; and incorporating PDAs into classes. For each of these initiatives to succeed, the campus infrastructure must be able to support it. Appendix C provides details about the campus IT infrastructure that makes these initiatives possible.

Campus IT Policies

University Policies

The University has developed and implemented the following campus-wide IT policies[9]. See Appendix A for further information on these policies.

- Academic Computer Use Policy
- Account Termination Policy
- Advertising Policy
- AntiVirus Policy
- Departmental Server Support Policy
- Disk Sanitizing Policy for Workstations
- ECU Network Use Policy
- ECU NT Domain Password Expiration Policy
- Email Purge Policy
- Network Scanning Policy
- Open Mail Relay Policy
- Spam E-Mail Policy
- University Student and Employee Computer Use Policy
- World Wide Web Policy

ITCS Policies

In addition to campus-wide policies, there are approximately 50 policies internal to ITCS that fall into the following categories:

- General Policies
- Organization And Reporting Structure
- Personnel
- General Administration
- Customer Services
- Data Management
- Security

- Operations

For a complete listing of the policy titles see Appendix B.

Technical Standards

EDP Audit

State and internal EDP audits are performed according to the COBIT (Control Objectives for Information and Related Technology) standards **[10]**. COBIT was developed as a generally applicable and accepted standard for IT security and control practices[1]. The main objective of COBIT is the development of clear policies and good practices for security and control in IT. ECU has adopted the COBIT standards for IT development, deployment, and maintenance.

Disaster Recovery Plan (DRP)/Business Continuity Plan (BCP)

ITCS developed a DRP/BCP template that provides departments and departmental server administrators with a standard for creating and maintaining their plans. In addition, this standard provides ITCS personnel, auditors, and other assessors a consistent format on which to review and test DRP/BCP documents and procedures.

ITCS Programming Standards Manual

ITCS Software Development Services maintains a standards manual that:

> *Provides a framework for development, support, operations, and maintenance of Administrative computer applications and services...Standards include project development processes, testing procedures, naming conventions, systems documentation, user documentation, training requirements, and other items relating to standard computing practices. The goal is to provide a guide that will result in a uniform, high quality level of service*[2].

Service Level Agreements

ITCS has established and documented a service level agreement (SLA) with each department that owns a server residing in the ITCS Operations Center. The SLA agreement identifies the scope of services provided by ITCS and those provided by the department or by outside service providers. Areas addressed include: policies and procedures, operating system and application support, security requirements, disaster recovery and business continuity planning, data backup and storage, and support response windows and times.

Student Computer Recommendations

ECU provides computing purchase recommendations for residence hall students **[11]**, Brody School of Medicine students **[12]**, and faculty/staff **[13]**. These recommendations address computing purchases for both campus and home use.

[1] From the *COBIT Framework Manual*.

[2] From the ITCS Software Development Services *Standards & Procedures Manual*

Supported Software and Hardware

ITCS maintains a list of supported software packages **[14]** that represents a set of computing tools designed to meet the needs of the University. Software and hardware support services include classroom and online workshops, consultant assistance with installations and use, and Help Desk assistance for front line questions.

Management Processes

Information Systems/IT Audit Performance

Following accepted auditing practice, ECU is periodically audited both by the Office of the State Auditor and ECU's Office of the Internal Auditor. The following assessments/audits were performed on ECU's electronic data processing (EDP) systems and processes:

1. Brody SOM, NC Office of the State Auditor, 1995
2. Brody SOM, KPMG Peat Marwick LLP, 1998
3. Brody SOM, General Controls, ECU Office of the Internal Auditor, May 1998
4. Brody SOM, Data Center, ECU Office of the Internal Auditor, August 1998
5. Brody SOM, Network, ECU Office of the Internal Auditor, January 1999
6. East Campus EDP Audit, ECU Office of the Internal Auditor, May 1999
7. Joyner Library, General Controls, ECU Office of the Internal Auditor, April 2000
8. Health Sciences Library, General Controls, ECU Office of the Internal Auditor, April 2000
9. Brody SOM EAD, ECU Office of the Internal Auditor, August 2000
10. Information Systems General Controls, NC Office of the State Auditor, May 2001

The University took appropriate actions to resolve the findings identified in each of these audits and is in compliance with accepted EDP practice. In the most recent state audit (Information Systems General Controls, NC Office of the State Auditor, May 2001), six reportable findings were identified. During the course of this audit the University took a proactive role. As the state auditors identified potential findings, the University took immediate action to resolve them. When the official report was released all six findings had been resolved.

In addition, the University has an internal auditor on staff that specializes in IT auditing. The services of this auditor have proven to be invaluable to the University in identifying areas of need and also as a resource to ITCS for monitoring compliance with COBIT during system design, implementation, and maintenance.

Acquisitions of Major IT Goods and Services

ITCS works in conjunction with the University's Materials Management Department to enter into centralized IT purchase contracts for the University. This covers all supplies, materials, printing, equipment, and service. ECU has capitalized on a centralized purchasing model for campus-wide IT equipment and software purchases such as workstations, servers, network equipment, and Microsoft products through volume discounts on State Term Contracts. In many cases, the large volumes and vendor relationships developed by the University are able to receive further discounts below standard educational prices. Items not on state contract are acquired by utilizing the following guidelines:

Item/Project costing $0 - $2,500

This purchasing range requires ITCS staff and other university departments to perform a competitive market analysis for products/services that meet our business needs. Bidding is not required.

Item/Project cost $2,500 - $5,000

This purchasing decision requires ITCS staff to obtain a minimum of three vendor quotes for centralized information technology purchases based on a competitive market analysis. For information technology purchases by other university departments, ITCS staff members are available to provide consulting on technology choices, maintainability and life cycle costs. Competitive bidding is not required.

Item/Project cost $5,000 - $25,000

This purchasing decision requires ITCS staff to define the scope, system requirements, and needs assessment for a product or service via the Systems Development Life Cycle document and bid by Materials Management via State of North Carolina Interactive Purchasing System. Even in case of a waiver of competition, if time permits, a written request for a quote will be sent out to the sole source. For information technology purchases by other university departments, ITCS staff members are available to provide consulting on technology choices, maintainability and life cycle costs.

Item/Project cost $25,000 - $100,000

This purchasing decision requires ITCS staff and applicable University committee to define the scope, system requirements, and needs assessment for a product or service via the Systems Development Life Cycle document and the appropriate committee process. The decision to provide this product, service, or function for campus has been evaluated and endorsed by the CIO prior to bid by Materials Management via State of North Carolina Interactive Purchasing System (IPS). For information technology purchases by other university departments, ITCS staff members are available to provide consulting on technology choices, maintainability and life cycle costs. The CIO must endorse the procurement of the product, service or function by university departments.

Item/Project cost $100,000+

This purchasing decision requires ITCS staff and all other university departments along with the applicable University committee to define the scope, system requirements, and needs assessment for a product or service via the Systems Development Life Cycle, appropriate committee process, and RFP document. The decision to provide this product, service, or function for campus has been evaluated and approved by the CIO prior to bidding. Items must be bid and awarded by the North Carolina Division of Purchase and Contract.

State Term Contracts

State Term Contract product guidelines are available online [15].

Major IT Project Implementation

The methodology used for determining major system acquisitions is the Systems Development Life Cycle (SDLC). Briefly, the SDLC is a defined study process that results in informed IT decisions. The process is summarized as follows.

> An individual or a group has a perceived need to automate a process. They make a request of the appropriate IT oversight committee permission to determine a solution. The committee assesses the need, approves the SDLC, and appoints the members of the study team, usually to include one or more members of the oversight committee and members of the group that has the need. The SDLC team performs a system requirement analysis in which the functionality of the solution is defined without regard for any product or existing process. In the case of a purchased solution rather than one which is custom programmed, the team begins soliciting information from prospective vendors.
>
> With this information in hand, it is then possible to assess short- and long-range costs and support needs, compatibility with other applications, as well as the impact on the servers, network, and other applications. The history and financial viability of vendors should also be assessed before the final decision is made.
>
> The SDLC is done in stages that are monitored by the oversight committee, and audit points are generated. The framework of the study is flexible enough to allow other issues to be addressed, such as assessments of liability as in the case of shadow patient records or student registration systems. It also allows input by resource people as needed, such as a compliance officer or an auditor. In effect, the SDLC has much in common with the purchase of any process solution; however, the potential for a negative impact on budget, support staff, computer and network systems, and compliance issues is far greater than buying a fancier officer copier. Therefore, it is necessary that the implementation of information systems solutions be accomplished through a standard process employing a team of knowledgeable persons.

IT Life Cycle Management

There are several major programs on campus that assist with the life cycle renewal of desktop and network infrastructures. These programs are funded at a level so that approximately 600 faculty and administrative desktops are replaced on a yearly basis, with individual desktop replacements occurring approximately once every 3 years. This allows desktop hardware to keep pace with the latest advances in software for faculty and students. Network infrastructure refreshes are based on General Administration Network guidelines for the UNC system. Reoccurring funds are provided from the Office of the President to maintain the baseline.

IT Professional Development And Training

ITCS has recognized the need for professional development of IT staff through developing and implementing the Staff Training and Education Program (STEP). The training program targets staff with skill development and serves as a recruitment tool. The training program also serves as a mechanism to retain top-caliber technology staff by providing a career enhancing training curricula with nationally recognized certifications. Individual staff wishing to participate in the training and certification program must complete an application and a development plan with their manager. The development plan includes goals, objectives, skills assessment; individual training curriculum, and specific projects to demonstrate skill competencies have been met. Curricula are based on the individual training needed to perform their jobs and a two-level certification program. Level 1-certification courses enable staff to become highly skilled in their field. The knowledge offered is structured to allow staff to build on their current experience and further develop their skills. Level 2 certification curricula exemplifies knowledge and skill sets that are indicative of someone who is highly proficient in their field of expertise and may be considered an expert. Each level will take 18 to 24 months to complete.

Participants are evaluated by data collected through monthly progress reports, project progression, course grades, skill assessment, evaluation meetings with a training coordinator, and their manager. Final evaluations are based on contents defined in the participant's development plan. Graduation from the program will be considered successful if the training program is completed within the specified timeframe (18 to 24 months) and participant has met course and project requirements as indicated in the development plan. ITCS currently has 27 participants in the training program with Level 1 Certification graduation scheduled for November 2003. The end result of this training program provides qualified staff that can meet the challenges of today's technology and thus enable ECU to stay in the technology race with other colleges and universities.

Disaster Recovery and Business Continuity Planning

ITCS maintains the Disaster Recovery Plan (DRP) for the University's critical IT applications. This plan identifies rapid response team members, procedures for establishing critical IT services at a remote hot site, and measures for returning critical IT services to normal operations. From the ITCS DRP:

> *The primary objective of the Disaster Recovery Plan is to help ensure the continued operation of our business by providing the ability to successfully recover computer services in the event of a disaster.*
>
> *Specific goals of the Plan relative to an emergency include:*
> 1. *To detail the correct course of action to follow*
> 2. *To minimize confusion, errors, and expense to the university*
> 3. *To perform a quick and complete recovery of services*
>
> *Secondary objectives of the Plan are:*
> 1. *To reduce risks of loss of services*
> 2. *To provide ongoing protection of university assets*
> 3. *To ensure the continued viability of this Plan*

The ITCS DRP is tested annually to ensure that offsite facilities and procedures are as needed. The latest test occurred in April 2002 and was performed successfully.

ITCS also provides space in the ITCS Operations Center for departmental servers performing critical university services. As a part of this service, ITCS requires that each department develop, maintain, and keep on file a DRP for their server. Department server DRP plans include such information as:

1. Nature and sensitivity of data
2. Operating system and version, application and version
3. Other systems on which the server depends
4. Location of business forms to be used as a backup method
5. DRP coordinator

In response to the 2001 State EDP Audit, University Financial Services developed disaster recovery and business continuity plans for each department within their unit. These plans were tested in conjunction with the April 2002 offsite disaster recovery test.

Assessment and Accountability

Assessment and accountability is an important component of the IT planning and implementation process. There are four major assessment methods employed by the central information technology organization as outlined below.

Customer Satisfaction Surveys

Upon completing service calls, ITCS technicians leave behind comment cards that address service quality and satisfaction. Return cards are tabulated and the results used to improve technical services in the field.

State EDP Audits

The Office of the State Auditor schedules audits of IT resources and processes on a four-year cycle. These audits are performed by a team of state auditors, and done so in close collaboration with ECU's Office of the Internal Auditor. These audits identify weaknesses in IT systems, as well as provide recommendations for resolving these weaknesses. The resulting audit reports represent a valuable resource for determining the strength of IT services, as well as a guide to improvement in assessments and controls.

Assessment Record Book

East Carolina University must demonstrate formal planning and evaluation within all of its administrative and educational support services. Each academic and administrative support unit prepares Assessment Record Book (ARB) documents that:

- Establish a clearly defined purpose that supports the institution's purpose and goals
- Formulate goals that support the purpose of each unit
- Develop and implement procedures to evaluate the extent to which goals are achieved
- Use the results to improve services

Each assessment record book specifically contains the following detailed information:

- Expanded statement of institutional purpose linkage
- Institutional mission/goal(s) reference
- Administrative or educational support unit mission statement
- Intended administrative objectives
- Each objective contains:
  - Means of unit assessment and the criteria for success
  - Summary of assessment data collected
  - Use of results to improve the unit's services

Assessment Record Books have been submitted by all academic degree programs and support units (including Information Technology and Computing Services) and are a continual process improvement mechanism used throughout East Carolina University. The Office of Institutional Effectiveness is responsible for coordinating the university's institutional effectiveness efforts including:

- Supporting faculty in the development and implementation of unit-based academic assessment protocols
- Assisting administrators and staff members in educational and administrative support units in the development of appropriate assessment protocols
- Providing staff support to the university institutional effectiveness committee
- Supervising staff and graduate assistants
- Creating an assessment library and resource center
- Supporting unit-based accreditation efforts
- Overseeing the university's continuing compliance with SACS accreditation criteria

Current planning and assessment practices will also be improved by establishing clearer ties between assessment and budgetary allocations.

SACS Reaffirmation

The Commission on Colleges of the Southern Association of Colleges and Schools (SACS) is the recognized regional accrediting body in 11 U.S. southern states (Alabama, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, South Carolina, Tennessee, Texas, and Virginia) for those institutions of higher education that award associate, baccalaureate, masters, or doctoral degrees.

An institution is required to conduct a self-study at the interval specified by the Commission (generally every 10 years) and, at the conclusion of the self-study, accept an honest and forthright peer assessment of institutional strengths and weaknesses. The Commission requires that the self-study assess every aspect of the institution. Also, the Commission requires an institutional follow-up plan to address issues identified in the self-study.

East Carolina University's Information Technology and Computing Services unit is also evaluated to ensure that all aspects of this unit are in full compliance with the SACS accreditation criteria. The 2000 Commission on Colleges of the Southern Association of Colleges and Schools' Criteria for Accreditation document outlines several key criteria for Information Technology including providing evidence that it is utilizing new technological advances into its operations; ensuring that appropriate resources support the planning function and the educational programs of the institution; ensuring that information technology is part of the curricula for its students; providing for ongoing training of faculty and staff in the use of technology; ensuring that policies are clearly written and followed for the allocation and use of information technology resources and are evaluated on a regular basis; and that all appropriate security measures are installed and monitored to protect the confidentiality and integrity of all administrative systems, academic systems, and institutional networks.

East Carolina University successfully met the information technology criteria for the SACS accreditation reaffirmation in March 2002.

Funding

The University provides both one-time and recurring funding for campus-wide IT projects through ITCS, the central IT support organization. One-time funding is obtained through a campus-wide reallocation procedure that occurs two to three times per year. This funding is used for projects that require substantially more funding on a one-time basis than is available in the recurring budget. Recurring funding is used for staff salaries, software and hardware maintenance, faculty workstation procurements to refresh the desktop technology every three years, staff training, test bed projects that are of limited scope, and other similar expenses.

A description of requested funding, in addition to requests for additional funding for new initiatives, is initiated by division level administrators and presented to the specific University Budget Committees charged with oversight of each specific budget. A matrix of the official ECU University Budget Committees and the State appropriated funding for which they are responsible is shown in the table below:

	Central IT	Division/ Department IT Academic Affairs	Division/ Department IT Health Sciences
Spending Authority	CIO	Unit Head/ Department Head	Unit Head/ Department Head
Review/ Consultation	IRCC	IRCC	Finance Committee (CISSC[3], MFPP[4])
Oversight	VC Admin and Finance	Provost	BSOM[5] Executive Committee/VC Admin and Finance

It should be noted that an accurate accounting is made of all funding resources and reports detailing how funds are expended are presented to university administrators and others as appropriate annually.

Additional information on the budget process may be found in the *SACS Self-Study Committee Report for Institutional Effectiveness*, Section 3.0.2 Budget Process **[16]**.

[3] CISSC is an acronym for Clinical Information Systems Steering Committee

[4] MFPP is an acronym for Medical Faculty Practice Plan

[5] BSOM is an acronym for Brody School of Medicine

Conclusion

East Carolina University has a robust IT infrastructure that includes: a central IT organization that provides a full range of computing services to the university community, gigabit network with high-speed connections to Internet and Internet2, an Operations Center housing nearly 200 systems in a physically secure environment, a help desk for faculty/staff and students, wireless connectivity, and a production web portal.

East Carolina University has a committee structure that is conducive to the collaborative development and approval of IT plans and activities. In addition, the University has formal processes for managing major IT purchases, developing and implementing IT initiatives, and for professional IT staff development and training. Also, the University has performed admirably with SACS assessments and EDP audits, as well as employs an internal IT auditor to conduct ongoing IT assessments and provide recommendations for improvement.

East Carolina University's strategic planning process is highly structured and tightly controlled, requiring the participation of all university planning units and departments. The University's operational IT plans, unit IT strategic plans, and the ECU strategic plan are inextricably linked through the planning and implementation process. This process requires cooperation and information sharing between academic, administrative, and healthcare units.

In summary, East Carolina University has an effective management staff and proven internal controls for the proper planning, acquisition, implementation, and delivery of information technology. East Carolina University exercises responsible stewardship of IT resources in pursuing its mission of service through education, research, and leadership.

East Carolina University, therefore, requests designation as a special responsibility constituent institution.

Bibliography

[1] **East Carolina University,** Strategies for Distinction: University Directions, 2000–2005, www.ecu.edu/pir/splan/StrategicPlanBk.pdf, 2000.

[2] **University of North Carolina Board of Governors,** Long Range Plan 2002 - 2007, http://www.northcarolina.edu/aa/planning/reports/longplan/LRP2002-07.pdf

[3] **University of North Carolina Office of the President,** A Roadmap to the Future: A Report to Faculty, Staff, Students, Trustees and Friends of the 16 Campuses, http://www.northcarolina.edu/ir/strategy/roadmap.cfm, 1998.

[4] **East Carolina University,** Planning and Institutional Research, www.ecu.edu/pir

[5] **East Carolina University,** Information Technology and Computing Services, Strategic Plan and Annual Report 2001-2002, www.ecu.edu/pir/splan/vpo/vpo 80001.pdf, 2002.

[6] **East Carolina University,** Information Resources Coordinating Council (IRCC), www.ecu.edu/ircc.

[7] **University of North Carolina Office of the President,** Information Technology Strategy for the University of North Carolina: Advancing Campus Computing and Collaboration, www.ga.unc.edu/its/netstudy/PHASE II/FINAL/ITS FINAL REPORT.pdf, 1999.

[8] **East Carolina University,** SACS Self-Study Committee Report, Section III Institutional Effectiveness, www.ecu.edu/sacs/SACS 2002/section III/sectionIIIreport.doc, 2002.

[9] **East Carolina University,** Information Technology Policies, www.ecu.edu/itcs/policies.

[10] **IT Governance Institute,** Control Objectives for Information and Related Technology, www.isaca.org/cobit.htm, 2000.

[11] **East Carolina University**, Residence hall student computer recommendations, http://www.studentstores.ecu.edu/RezNet.html.

[12] **East Carolina University,** Brody School of Medicine student workstation recommendations, www.studentstores.ecu.edu/medicalsales.html.

[13] **East Carolina University,** Faculty/staff workstation and server recommendations, www.ecu.edu/itcs/purchasing computers.cfm.

[14] **East Carolina University,** Supported software and hardware, www.ecu.edu/itcs/software sup.cfm.

[15] **North Carolina Purchase and Contract,** State term contract product guidelines, www.doa.state.nc.us/PandC/.

[16] **East Carolina University,** SACS Self-Study Committee Report, Section 3.0.2 Budget Process, www.ecu.edu/sacs/SACS 2002/section III/sectionIIIreport.doc, 2002.

[17] **University of North Carolina Office of the President,** UNC Network Assessment Minimum Network Specifications, www.ga.unc.edu/its/netstudy/netspec.html, 2000.

[18] **North Carolina Research and Educational Network**, Logical network map, www.ncren.net/Internet/data.html.

[19] **East Carolina University,** Wireless networking, www.ecu.edu/wireless/.

[20] **East Carolina University**, Instructional Technology Consultants, http://core.ecu.edu/vel/itc/.

[21] **East Carolina University**, University Multimedia Center, http://core.ecu.edu/umc/mission.htm.

[22] **East Carolina University**, Center for Interdisciplinary Instructional Technology Research (CIITR), www.ecu.edu/ciitr/default.htm.

[23] **East Carolina University**, Reconfigurable Advanced Visualization Environment (RAVE), www.ecu.edu/ciitr/rave.htm.

Appendix A – University IT Policies

Academic Computer Use Policy

Purpose of Policy: To govern the use of University computer systems, which includes hardware, data, software and communications networks.

Person(s) with Primary Responsibilities: Chief Information Officer

Approved: Chief Information Officer

General Statement:
Freedom of expression and academic freedom are limited to no greater degree in electronic formats than in printed or oral communication. Individual faculty members are entitled to full freedom in research and in the publication of results. Academic freedom includes freedom of artistic expression through electronic means as well as in familiar and traditional media. Intellectual property in electronic form is as fully protected as are those properties in other forms. Individual faculty members are entitled to freedom in the classroom in discussing their subject, including those formats used in virtual spaces and areas where communication is inherent in the teaching and learning process.

The University provides academic access to a functioning system of electronic communication on a nondiscriminatory basis, without regard to the perceived merit of a particular content or subject matter or the views of users. Equality of access is assured without regard to race, gender, nationality, age, religion, disability, or sexual orientation.

The University relies heavily upon its computer information systems to meet operational, financial, educational and informational needs. It is essential that East Carolina University's computer systems, and computer networks, as well as the data they store and process, 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.

This policy applies to University computer systems and refers to hardware, data, software 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 network.

Individual faculty members shall make every effort to show that they are not speaking for the University when they are not. Special care shall be taken in posting or distributing digital material, on a web page or site created and accessed through the University computing system. Individual faculty members must avoid or dispel any inference that the speaker represents the views of the University or of faculty colleagues. Individual faculty members are responsible for following federal, state, University of North Carolina Board of Governors, and University laws and policies.

Regulatory Limitations:

The University may monitor access to the equipment and networking structures and systems to insure the security and operating performance of its systems and networks and to enforce University policies. Monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

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.

The University may authorize confidential passwords or other secure entry identification; however, employees 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. Again, monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

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.

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

Permissible Uses:

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

1. The use is lawful under federal or state law.
2. The use is not prohibited by Board of Governors, University, or institutional policies.
3. The use does not overload the University computer equipment or systems, or otherwise harm or negatively impact the system's performance.
4. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies.
5. The use does not violate federal or state laws or University policies on copyright and trademark.
6. The use does not state or imply University sponsorship or endorsement.
7. The use does not violate state or federal laws or University policies against race or sex discrimination, including sexual harassment.
8. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security in any way attempts to gain unauthorized access.

Other Computer Usage Guidelines:

Users are to have valid, authorized accounts and may only use those computer resources that are specifically authorized. Users are responsible for taking reasonable precautions to safeguard their own computer account.

Users who choose to publish home pages on the World Wide Web must identify themselves as the author. In addition, they must include a disclaimer that any personal home page content reflects their own views and not necessarily that of the University. Furthermore, any links to other web resources must be identified.

Users may not change, copy, delete, read or otherwise access files or software owned by other parties without permission of the custodian of the files or the system administrator. Users may not bypass accounting or security mechanisms to circumvent data protection schemes. Users may not attempt to modify software except when intended to be user customized.

Users shall assume that any software they did not create is copyrighted. They may neither distribute copyrighted proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.

Users must not use the computer systems to violate any rules in the East Carolina University Faculty Manual, or any local, state or federal laws.

University policies stated in the Faculty Manual of which individual faculty members should be aware that may bear on computer use include Part IV, Section V, External Professional Activities for Pay; Part VII, Section II.G., Copyright Procedures; Appendix I, East Carolina University Policy on Conflicts of Interest and Commitment.

North Carolina statutes of which individual faculty members should be aware that may bear on computer use include §14-190-1, Obscene Literature and Exhibitions; §114-15.1. Denial of Computer Services to an Authorized User; §114-14.1 Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation. United States statutes of which individual faculty members should be aware that indirectly may bear on computer use include Title 18, Section 1030, Fraud and Related Activity in Connection with Computers.

Account Termination Policy

Purpose of Policy: The purpose of this policy is to ensure that the supervisor of an employee leaving the University notifies ITCS, so that user access to core IT resources can be revoked in a timely manner. This policy is concerned with terminated employees that have update access to critical or sensitive information.

Person(s) with Primary Responsibilities: Primary responsibility belongs to the supervisor of the employee leaving the University.

Approved: Chief Information Officer:

General Statement:
The supervisor of a terminated employee must notify ITCS of the separation on or before the employee's termination date so that account access can be revoked appropriately. The supervisor must notify ITCS by submitting a service request to IT Support Services by the online service request system (www.ecu.edu/itcs/helpdesk) or by telephone at 328-6866 and provide the employee's user account IDs and other identifying information (name, department, social security number, etc).

Upon receiving notification from the supervisor of a terminated employee, the security administrator will call the supervisor for verification before revoking the employee's account access.

Advertising Policy

Purpose of Policy: Prohibiting Commercial Advertisements that Use University Media

Person(s) with Primary Responsibility: Chief Information Officer

Approved: Chief Information Officer

General Statement:
It is the policy of East Carolina University that University media that utilize funds appropriated by the State may not be used for commercial advertising. Commercial advertising includes any advertising or promotion provided in exchange for legal consideration including money or other valuable benefits. The University may acknowledge sponsors, provided such acknowledgment does not include qualitative or comparative language, price information or other indications of savings or value associated with any product or service; call to action; endorsements; or any inducement to buy products. Acknowledgment in the following form is permissible:

Websites:
University media include all University websites with a worldwide web address that are sponsored or endorsed or created on authority of a University department or administrative unit and that reside on University servers or have an ecu.edu domain name. Personal websites maintained by University computer users on University servers may not contain paid advertising. University computers may not be used in a manner that results in commercial gain or private profit except as allowed under University intellectual property policies.

E-mail Broadcasting:
The University will not permit the use of the E-mail system for personal or commercial advertising, profit or gain.

Trademarks:
The University's registered trademarks may not be used in any manner that misleads or confuses the public concerning University sponsorship of any publication or project, event, or other undertaking. The University's registered trademarks may not be used for commercial purposes except as authorized under the University's Licensing Program.

Linking:
No graphics or other links from University websites or personal websites residing on University servers or that have the University domain name may be used for commercial advertising. Logos for software used to create a website are permitted to appear on the site. It is permissible for University computer users to link with an outside site for legitimate educational or charitable purposes.

AntiVirus Policy

Purpose of Policy: To prevent infection of University computers and computer systems by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to user applications, files, and hardware.

Person(s) with Primary Responsibility: Director of IT Security

Approved: Chief Information Officer

Antivirus Policy:
All Windows and Macintosh computers (clients and servers) connected to the East Carolina University computer network (herein referred to as "the network") or networked resources shall have ITCS-supported antivirus software (preferably the most current version) correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network. If deemed necessary to prevent viral propagation to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code (herein collectively referred to as "virus" or "viruses") shall be disconnected from the network until the infection has been removed.

If a Windows or Macintosh computer does not have ITCS-supported antivirus software installed, it shall be installed according to one of the two following methods:

- If the installation source is a University-distributed CD-ROM, the antivirus software shall be installed before establishing any connection to the network. Upon establishing the initial network connection, the virus definitions shall be updated to the most current version immediately and before loading or installing any other software or data.
- If the installation source is a University server, the computer shall be connected to the network for the sole purpose of installing antivirus software from that server. The installation shall be performed immediately upon establishing the initial network connection and virus updates downloaded and installed before loading or installing any other software or data.

Under all other circumstances, any Windows or Macintosh computer connected to the network shall have ITCS-supported antivirus software properly installed, configured, and updated before being connected to the network.

ITCS strongly advises that:

- Virus definitions should be updated daily before retrieving email.
- All files on all hard drives should be scanned weekly.

Directions for automating these processes are located at http://www.ecu.edu/itcs/micro/NAVInstructions.pdf. When an enterprise-wide virus attack is in progress, ITCS shall notify the campus computing community via the best available method and all files on all hard drives should be scanned immediately using the newest virus definitions available.

Other operating systems or computing platforms shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available.

When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network. Any exceptions to this policy must be explicitly approved by the ITCS Information Technology Security Department.

Justification and Rationale:

Availability, performance, and security of the network represent essential core assets to the daily operation of the University. Viruses and other forms of malicious code (worms, trojans, backdoors, VBS scripts, mass-mailers, etc.) represent a significant threat to these assets. In order to combat this threat, a comprehensive enterprise security policy must include antivirus provisions to detect, remove, and protect against viral infections. Antiviral procedures should include identification of current and potential viral threats, computers and systems at risk of infection, files at risk of infection, infected computers, and infected files. Infection patterns should be tracked and analyzed to identify chronic internal and external threats.

Many virus infections threaten other computers sharing the infected computer's network. Infected computers must be cleared of viral infections immediately. Files that can be cleaned should have the viral code removed, thus returning them to pre-infected state. Files that cannot be cleaned must be quarantined until such time as they can be replaced with uninfected copies. If all efforts at removing viral infection fail, the computer's hard drive must be formatted and all software reinstalled using clean licensed copies. If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer must be disconnected from the network until it is serviced by an ITCS representative or designee who will verify that the computer is virus-free.

Antivirus activities must be centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. Users must be educated about viral threats and the computing practices required to protect against infection. Whenever a new viral threat appears, the user community must be warned about the new threat. Up-to-date antivirus software must be distributed and its availability advertised to the University community.

Established Antiviral Procedures:

Every year, ITCS purchases a site license for Symantec Norton AntiVirus (NAV) to protect University computers and systems from virus infections. Computers purchased for large-scale rollouts are delivered with NAV already installed. Whenever ITCS personnel setup a new computer, they ensure that NAV is installed before or immediately upon connecting the computer to the network.

The site license permits ECU faculty, staff, and students to have NAV on all Windows and Macintosh computers on the ECU campus. The site license also contains provisions allowing ECU faculty, staff, and students to install NAV software on their home computers free of charge. ITCS distributes NAV software as follows:

- Campus users can request NAV program installation on campus computers by contacting IT Support Services.
- Users can install NAV from CD-ROM on their computers on campus and at home. ITCS distributes NAV on CD-ROM via established conduits, which are continually advertised to the University community.
- Users on- and off-campus can install NAV via the Internet from the secure ITCS website.

Distributed software includes documentation for proper installation, configuration, and use of the software (including instructions for automating file scanning and virus definition updates). ITCS maintains a well publicized user-oriented website containing this documentation at http://www.ecu.edu/itcs/micro/NAVInstructions.pdf. Symantec provides free incremental updates of program code and virus definitions via the LiveUpdate utility built into NAV. In short, everyone connected with ECU has easy access to a free copy of NAV, NAV updates, and NAV documentation.

IT Support Services provides end-user support and forwards virus-related service requests (coded with high priority by default) to the appropriate group for rapid response. The Workstation Support Group and Critical Applications Support provide second-level user support to East and West campuses respectively. Individual server administrators provide antivirus support for servers. IT Security provides enterprise-level antivirus support and coordination of rapid responses to enterprise-level virus attacks.

Departmental Server Support Policy

Purpose of Policy: With the growth of distributed processing at East Carolina University and the need to support educational, research and other specific applications, there is a concomitant growing need for file and application servers. This policy is intended to provide guidance to departments who are considering the installation of their own servers and to define the conditions that must be met in order that ITCS/Informatics provide support for those servers.

Administrative Responsibilities: The ECU Departmental Server Policy will be administered by the IT Consulting Server Group. Issues of non-compliance with this policy will be assessed by the IT Consulting Server Group and referred to the Chief Information Officer for action.

Approved: Chief Information Officer

Guidelines:

Physical, Environmental, and Security Controls for departments with servers

1. Each department must have a person trained to administer their network operating system (NOS) and a backup or an access agreement for a backup for that person. For specifics about the NOS and training needed for certification please contact ITCS.
2. Each department will ensure that scheduled backups of the file server data and applications are routinely completed.
3. The file server and documentation will be located in a secure area and access restricted to authorized personnel.
4. Each department will file with ITCS an appropriate disaster recovery plan using the template provided by ITCS.
5. File server equipment will be protected from the effects of electrical surges and outages by having an uninterruptible power supply (UPS) attached to the server.
6. Up-to-date information about all communication lines interconnected to the outside 'net' should be maintained.
7. File server and data access permissions should be established for the appropriate users only.
8. Servers must meet ITCS hardware and NOS specifications. Specialized rack/network configurations must be purchased if departments choose to utilize the ITCS Computer Operations facility.
9. Departments will be responsible for purchasing maintenance contracts from the software vendor for departmental-specific software.

Domain Controls

ITCS and Informatics are discourages the establishment of domains other than ECU and Info-1. By definition, a domain is a logical grouping of network servers and other computers that share common security and user-account information. Within domains, administrators create one user account for each user. Users then log on to the domain, not to individual servers in the domain. Guidelines are as follows:

1. Separate domains installed prior to a formal or stated policy to the contrary will continue to be supported by ITCS. Departmental administrators will have full administrative control over these servers as well as consulting and technical support from ITCS.

2. New domains may be established only after appropriate coordination with ITCS has clarified operational, connectivity and support issues for the new domain.

3. New trust relationships will be established with the ECU or Info-1 domains from separate domains when appropriate coordination with ITCS support staff has been made. Any new domains meeting the security and trust requirements of ITCS must utilize the existing user identification schema provided by ITCS.

Hardware/Software Controls

As hardware and software requirements are subject to change, a list of the current hardware/software requirements can be obtained at http://www.ecu.edu/ITCS/client_serv.html

Further Information:

If you have questions or need clarification on this policy please contact the Director of IT Consulting.

Disk Sanitizing Policy for Workstations

Purpose of Policy: To maintain data confidentiality by preventing access to information previously stored on workstations transferred to new users or destined for surplus.

Person(s) with Primary Responsibility: Managers of (1) Workstation Support Group (WSG) and (2) Critical Applications Support (CAS)

Approved: Chief Information Officer

Disk Sanitizing Policy: Whenever a state-owned Windows or Macintosh workstation is sent from ECU to surplus, the non-removable hard drive(s) shall be "sanitized" (i.e., all data removed in a manner that prevents subsequent recovery) before the computer leaves the ECU campus. Sanitizing shall be performed by qualified personnel from Workstation Support Group (WSG) and/or Critical Applications Support (CAS).

Whenever a state-owned workstation is transferred from one primary user to another without leaving the ECU campus, the hard drive shall be sanitized as soon as the original user's data has been removed. The appropriate operating system and applications shall be installed with default settings before delivery to the new user.

The software used to sanitize hard drives shall be approved by ITCS and comply with applicable security guidelines established by the United States Department of Defense. Users should ensure that data covered by the North Carolina Records Retention Policy is copied from computers and appropriately stored before their disks are sanitized.

Procedure:

Before leaving the ECU campus, workstations delivered to central surplus shall be sanitized by WSG and/or CAS representatives using one of the following procedures.

- If the computer will boot and all its internal hard drives are accessible by sanitizing software, the hard drives shall be sanitized using ITCS-approved software.
- If the computer will not boot and/or all its internal hard drives are not immediately accessible by sanitizing software, the hard drives shall be rendered permanently inoperative via physical or magnetic destruction. The system unit shall be marked as containing a non-functional hard drive.

Justification and Rationale:

ITCS expends substantial time, effort, and funding to protect the confidentiality of data stored on computers on the ECU campus. However, every year, ECU sends many computers to surplus. These computers contain information that must be kept confidential—application data, licensed software, licensing keys, passwords, email, and other sensitive information. Deleting selected files from the computer and even formatting the hard drive(s) does not prevent subsequent recovery and use of this information by unscrupulous individuals using commonly available applications.

The U.S. Department of Defense has established guidelines for permanently erasing hard drive information and eliminating its recovery. DOD 5220.22 requires that all non-removable hard drives must be sanitized for reuse by overwriting all addressable locations with a character, its complement, then a random character and verification.

Commercially available applications can delete all information from a computer hard drive and repeatedly overwrite its entire surface, thus defeating any subsequent attempts at recovering the formerly stored information. One such application is CleanDrive from White Canyon Software, which complies with DOD security specifications and is currently used by ITCS for disk sanitizing.

ECU Network Use Policy

Purpose of Policy: To establish guidelines governing the use and connection of networking devices on the University's Data Communications Network. This policy applies to all University networked devices, ranging from multi-user systems to single user personal computers. This includes networked printers, mini-hubs, routers, switches, and any other network communication devices, which are connected to the University's network

Person(s) with Primary Responsibility: Director of IT Services.

Approved: IRCC and ISSC

Policy: The University provides network access and capabilities through the Information Technology Services Team of the Information Technology and Computing Services Department. The guidelines listed below are required in order to provide the University a reliable and stable networking platform.

Guidelines:
All networking equipment connected to the University network must first be registered and approved by the Information Technology Services Team of the Information Technology and Computing Services Department. The responsible parties of problem network devices and/or services will be notified and expected to correct the problem in a timely manner.

Any networked devices or services that are detected and verified to degrade the quality for service on the network, if not corrected will result in termination of network service of that device until the cause of the problem is corrected.

Activities, which interfere with the operation of the network, are prohibited. These include but are not limited to the propagation of computer worms, network sweeps, network probing, viruses, or Trojan horses.

Violations:
Violations will result in the termination of network service to the offending network device and in the case of a willful violation be handled in accordance with either the ECU Academic Computer Use Policy or the ECU Student and Employee Computer Use Policy. Network abuse will be referred to the Chief Information Officer, and/or Director of Information Technology Services.

ECU NT Domain Password Expiration Policy

Purpose of Policy: This policy defines the procedures for the expiration of passwords for ITCS enterprise systems. This policy affects the use of ITCS maintained mainframe systems and enterprise servers. This policy has been designed to meet N.C. State audit requirements, governing access to sensitive data.

Person(s) with Primary Responsibilities: The Director of IT Services is the primary person charged with administering the ITCS Password Expiration Policy. The systems administrators for the ITCS enterprise systems will be responsible for the notification and expiration of passwords.

Approved: Chief Information Officer

General Statement: Passwords on ITCS enterprise systems will expire on a regular basis, currently no longer than ninety (90) days, with notification to users via e-mail or system messaging at least 3 times in the two weeks prior to expiration. The only exceptions to this policy are those systems that do not have the capability to force password changes.

Email Purge Policy

Purpose of Policy: To establish guidelines for automatic removal of older mail items in the Inbox, Sent Items, Calendar, and Deleted Items folders. Automatic purging will maintain the client databases, limit disk space usage, and reduce possible corruption.

Approved: Information Systems Steering Committee (ISSC) and Information Resource Coordinating Council (IRCC).

Person(s) with Primary Responsibilities: Primary responsibility belongs to the Chief Information Officer.

Database Purges:

Inbox - 120 days: The Inbox is the primary folder for all incoming mail items. Items that are older than 120 days will automatically be deleted. These items will be placed in the Deleted Items folder for up to seven days.

Sent Items- 120 days: The Sent Items is the folder that contains all outgoing mail items. Items that are older than 120 days will automatically be deleted. These items will be placed in the Deleted Items folder for up to seven days.

Calendar - 180 days: Appointments, Tasks, and Notes that are older than 180 days will automatically be deleted. These items will be placed in the Deleted Items folder for up to seven days as indicated below. Reoccurring appointments will only be removed from the calendar if they meet the 180-day criteria.

Deleted Items - 7 days: The items that are marked for deletion are placed in the Deleted Items folder for seven days. Afterward, the items will be automatically removed. These items cannot be restored easily; therefore it is critical to mark only the items that need deleting.

In order to maintain mail past the date limitations, establish automatic archiving to a specific directory on your personal computer or within another folder in your mailbox before the dates indicated above. Please reference HELP in the particular email client for assistance.

Network Scanning Policy

Purpose of Policy: To prohibit the use of the University's computers, electronic communications, or other information technology resources to perform network-based scans on any computing system without the written permission of the system owner or system administrator.

Person(s) with Primary Responsibilities: Primary responsibility belongs to the Chief Information Officer. The Director of IT Security will coordinate technical investigations of network scanning incidents.

Approved: ISSC on April 3, 2001, and IRCC on April 25, 2001

General Statement: It is the policy of East Carolina University that no computer system procured or managed by the University or connected to the University's network shall be used to perform network scans on *any* computer system, except under the following conditions:

- A system may be scanned by the owner or the system administrator of that system.
- A person may scan a system on behalf of another only after receiving written permission signed and dated by the owner or system administrator of that system. This document shall include a specific time period during which the scan(s) may be performed. Any additional scanning shall require separate written approval.
- The University network and system staff may perform network scans in an effort to resolve a service problem, as a part of normal system operations and maintenance, or to enhance the security of the systems that they manage.
- The University IT security staff and internal auditing staff may perform network scans to monitor compliance with University policy, to perform security assessments, or to investigate security incidents.

Definitions:

Network Port: A numeric identifier used to distinguish between different network services (i.e., HTTP, Telnet, FTP) on the same computing system. Although port numbers range from 0 to 65536, many well known services have reserved port numbers between 0 and 1024 (i.e., HTTP uses port 80, Telnet uses port 23, and FTP uses ports 20 and 21.) To establish a session with a host, a network request must be sent to the appropriate port number on the host. That is, to establish an HTTP session with a web server, your workstation software will send a request to port 80 of the web server.

Network Port Scanning: The process of sending data packets over the network to selected service port numbers (HTTP-80, Telnet-23, etc.) of a computing system with the purpose of identifying available network services on that system. This process is helpful for troubleshooting system problems or tightening system security. Network port scanning is an information gathering process, and when performed by unknown individuals it is considered a prelude to attack.

Vulnerability Scanning: The process of identifying known vulnerabilities of computing systems on the network. This process goes a step beyond identifying the available network services of a system as performed by a network port scan. The vulnerability scan will identify specific weaknesses in the operating system or application software, which can be used to compromise or crash the system. Vulnerability scanning is intrusive and should be performed with care, as some scans can cause systems to crash or to behave erratically. The vulnerability scan is also an information gathering process, and when performed by unknown individuals it is considered a prelude to attack.

Network Scanning: The use of a computer network for gathering information on computing systems, which may be used for system maintenance, security assessment and investigation, and for attack. This includes network port scanning and vulnerability scanning.

Threats to University Information and Information Resources:

Network scanning—if used properly--is a formidable tool for protecting our information and information resources. On the other hand, unauthorized network scans pose a serious threat to the availability, integrity, and confidentiality of our electronic information and our information resources.

Unauthorized network scans can result in:

1. **Disclosure of Sensitive Data:** Network scans yield a tremendous amount of information about our networked computing systems. This information is crucial to attackers in their efforts to compromise computer systems. If a critical system is compromised, an attacker may have unlimited access to confidential data.

2. **Loss of Service:** Network attacks vary greatly in nature. The goal of the attack may be to gain control of a computing system or to simply make the system unavailable to others. Even the process of vulnerability scanning can cause a system to crash or behave erratically.

3. **Loss of Network and System Performance:** Network scanning can involve hundreds or even thousands of computing systems. The sheer volume of network traffic requests can place an incredible strain on the resources of our computing systems and the University network, resulting in less than optimal performance for University users.

4. **Loss of Reputation:** As a member of the global Internet village our actions directly affect the safety of information and information resources around the world. By allowing the University's computing resources to be used to compromise systems belonging to our global neighbors, our reputation as a responsible member of Internet will be tarnished.

Violations:

Violations of this policy will be addressed as violations of the "Academic Computer Use Policy" and the "University Student and Employee Computer Use Policy."

Open Mail Relay Policy

Purpose of Policy: To prohibit the use of open mail relay on University computer systems.

Person(s) with Primary Responsibilities: Primary responsibility belongs to the Chief Information Officer. The Director of IT Services will coordinate technical investigations of open mail relay incidents and assist with subsequent technical solutions.

Approved: ISSC on January 9, 2001, and IRCC on January 24, 2001

General Statement: It is the policy of East Carolina University that no computer system procured or managed by the University or connected to the University's network shall run an open mail relay.

An open mail relay is a computer system that accepts and routes any email it receives without authenticating the sender. This feature was needed in the early days of the Internet to relay email from one system to another and on to its destination. However, this cooperative arrangement was eventually exploited. The email system owners soon found themselves distributing large volumes of unsolicited commercial email, known as spam, on the behalf of others and at their own expense.

Although few email servers today require open mail relay, many systems still include it as a base feature. Unfortunately, open mail relay is often activated during the install process by a novice email administrator or by a busy technician using default installation settings. Spam mailers are constantly scanning Internet for these systems and will frequently find and exploit a new open mail relay system in a matter of days.

The impact of running open mail relay on a University system is manifold. The consequences include:

1. **Blacklisting:** In an effort to curb the spread of spam some groups, such as Mail Abuse Prevention System (MAPS), maintain a blacklist of sites that operate open mail relays. Individual site administrators frequently use these blacklists to block email originating from open mail relay sites, and in some cases will block all network traffic (i.e., web, FTP, telnet). This results in legitimate, University email and network traffic being blocked at the destination site.
2. **Performance Degradation:** Receiving, storing, and delivering large volumes of non-University email messages place an undue strain on the resources of our email systems. Memory, disk space, CPU cycles, as well as Internet bandwidth are consumed, resulting in less than optimal performance for University users.
3. **Loss of Service:** The volume of spam can be great enough to render an email server inaccessible or cause it to crash.

4. **Unnecessary Cost:** The cost of processing, storage, and distribution of spam email requires more server hardware, network bandwidth, and support time than it would otherwise.

5. **Loss of Reputation:** Providing email distribution services to spammers tarnishes the University's reputation as a responsible member of Internet. The Internet Society rejects the use of open mail relay systems in their Best Current Practices documents, Request for Comments (RFC) 2505 and 2635.

Spam E-Mail Policy

Purpose of Policy: This policy defines the procedures for handling violations of the Academic Computer Use Policy and the University Student and Employee Computer Use Policy in cases involving spam email. It also describes procedures to use when a non-university account sends a spam message to a university account.

Person(s) with Primary Responsibilities: The Chief Information Officer is the primary person charged with administering the spam email policy. The systems administrator for Exchange is the person who will remove the computing resource access privileges when directed to do so by the CIO. The Director of IT Consulting will coordinate the suspension and reinstatements of accounts. ECU faculty, staff and students are responsible for recognizing and reporting violations of the policy to the Help Desk.

Approved: Chief Information Officer

General Statement: This policy is written to conform to the requirements and procedures of the Academic Computer Use Policy and the University Student and Employee Computer Use Policy. These policies state that faculty, staff, and students may use the University's email system as long as the use does not overload the University computer equipment or systems, or otherwise harm or negatively impact the system's performance by excessive use of computing resources. This spam mail policy prohibits the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via email to a group of persons not requesting the message except when conducting official university business.

Violation of Policy by University Employees: Any violation of these computer use policies is "misconduct" under EPA policies (faculty and EPA non-faculty) and "'unacceptable personal conduct" under SPA policies. Sanctions for violation of this policy may include one or more of the following: a written warning, a revocation of access privileges; a written reprimand; demotion; suspension without pay; or dismissal. Violations of law may also be referred for criminal or civil prosecution.

> **Action to be Taken:** On the first occurrence, the offending employee will be notified in writing or by email of a violation of this policy, will be reminded of the clause in the University Student and Employee Computer Use Policy that prohibits overloading, harming or negatively impacting the system's performance, and will be advised that a subsequent occurrence will result in suspension of email privileges.
>
> If further occurrences are reported, the employee's unit administrator will be notified of the violation and the email account will be disabled pending further investigation. The unit administrator can request a reinstatement of the account from the ITCS Director of IT Consulting. If the violation warrants further action, the unit administrator will notify the Department of Human Resources. Any other sanctions imposed will follow the existing unacceptable personal conduct procedures of the University.

If the situation is severe enough to threaten the integrity or performance of the system in the judgment of the CIO, even on the first occurrence, the email account may be disabled for as long as it takes to eliminate the threat.

Violation of Policy by Students: Any violation of this policy is "misconduct" under the University's student conduct code. Violations should be reported as provided in that code. 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. Violations of law may also be referred for criminal or civil prosecution.

Action to be Taken: On the first occurrence, the offending student will be notified in writing or by email of a violation of this policy, will be reminded of the clause in the University Student and Employee Computer Use Policy that prohibits overloading, harming or negatively impacting the system's performance, and will be advised that a subsequent occurrence will result in suspension of email privileges.

Upon subsequent occurrences, the student's name will be forwarded to Student Life's Associate Dean of Students, along with an explanation of the offense. The student's account will be disabled until Student Life authorizes reinstatement through the ITCS Director of I.T. Consulting.

Student Life will determine whether to disable the student's account for any length of time and then only after going through the procedure proscribed under the student conduct code policy.

Violation of Policy by Faculty: Any violation of these computer use policies is "misconduct" under EPA policies.

Action to be Taken: The offending faculty member will be advised in writing or by email of the clause in the Academic Computer Use Policy that prohibits overloading, harming, or negatively impacting the system's performance.

The faculty member's department chair will be notified of the occurrence.

If the situation is severe enough to threaten the integrity or performance of the system, the CIO or an appointed representative will authorize the account's removal. The account will be disabled for as long as it takes to eliminate the threat.

Additional Steps to be Taken to Minimize Spam Mail Incidents: The number of addresses that can be included in the header of an Exchange email should be limited to 300 items. This maximum should be large enough to allow for normal business email while reducing the severity of cases of spam policy violation.

A campus-wide effort will be made to educate all users about the harmful effects of sending "spam" mail and indiscriminately using the "reply to all" function.

The faculty and student/employee policies along with the procedures for handling violations as stated above will be publicized in the East Carolinian, somewhere within the ECU web pages, in Pieces of Eight, and posted in resident halls and labs.

Spam Mail from Non-University Accounts:

Spam mail coming from non-university accounts can also be detrimental to our systems and are not welcomed by our users. We must be able to take steps to keep these problems to a minimum.

Action to be Taken:

On the first occurrence, the sender will be notified that spam mail should not be sent to university accounts and that any further receipt of such messages will initiate our procedures to block email coming from the sender's account.

On the second occurrence, the system will be configured to block email coming from the offending account. Any reinstatement of privileges must be requested from the ITCS Director of IT Consulting.

University Student and Employee Computer Use Policy

Purpose of Policy: To govern the use of University computer systems, which includes hardware, data, software and communications networks.

Person(s) with Primary Responsibility: Chief Information Officer

Approved: Chief Information Officer

I. This policy applies to all university students and employees whether full time, part time, temporary, or volunteer, but excludes faculty who are governed by the Academic Computer Use Policy.

A. Freedom of expression is limited to no greater degree in electronic formats than in printed or oral communication. Individual employees or students are entitled to full freedom in research and in the publication of those results to include freedom of speech and freedom of artistic expression through electronic means as well as in familiar and traditional media. Electronic means of freedom includes the respect for open forum communications free of harassment and discrimination. Intellectual property in electronic form is as fully protected as are those properties in other forms. It is important for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

B. The University provides academic access to a functioning system of electronic communication on a nondiscriminatory basis, without regard to the perceived merit of a particular content or subject matter or the views of users. Equality of access is assured without regard to race, gender, nationality, age, religion, sexual orientation, or disability.

C. The University relies heavily upon its computer information systems to meet operational, financial, educational and informational needs. It is essential that East Carolina University's computer systems and computer network, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is also critical that these systems and machines be protected from misuse and unauthorized access. It is the individual user's responsibility to safeguard passwords on personal computers from unauthorized use. To that end, University employees and students are expected to act reasonably and in a responsible manner involving their usage of computing resources. This includes sensitivity to excessive computing resource use as in mass-email distribution or consumable supplies such as paper. University employees and students who willfully engage in the degradation of or intent to damage such computing resources will be subject to such action as deemed appropriate by University administration in accordance with University policy and any applicable state or federal laws.

D. This policy applies to all University procured and managed computer systems including hardware, data, software, and the communication networks associated with these computers. In addition, this policy applies to all non-university owned computers connected to the University's network and to all users of computing resources owned or managed by the University, including, but not limited to, University employees, students, guests of the administration, external individuals or organizations and individuals accessing University computing resources through external network services, such as the Internet.

E. Individual employees and students shall make every effort to show that they are not speaking for the University when they are not. Special care shall be taken in posting or distributing digital material, on a web page or site created and accessed through the University computing system. Individual employees and student members must avoid or dispel any inference that the speaker represents the views of the University or of employees and student colleagues.

F. Individual employees and students are responsible for following federal, state, University of North Carolina Board of Governors, and University laws and policies.

II. Regulatory Limitations

A. The University reserves the right to limit employee and student computing resource access when federal or state laws or University policies are violated or when University contractual obligations or University operations may be impeded.

B. The University may authorize confidential passwords or other secure entry identification; however, employees and students have no expectation of privacy in the material sent or received by them over University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above.

C. The University has the right to monitor network traffic, including electronic mail (e-mail), to and from privately owned machines connected to the University network within the limitations described above. 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. However, if University Administration is informed of inappropriate employee or student conduct as associated with computing resource use, it is obligated to investigate and to enforce applicable federal, state, University of North Carolina Board of Governors, and University laws and policies.

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

E. The University may monitor access to the equipment and networking structures and systems to insure the security and operating performance of its systems and networks and to enforce University policies. Monitoring or otherwise accessing of individual employee and student computers to enforce University policies requires specific approval of the Chancellor.

III. Permissible Uses

A. Employees and 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.

B. Employees and students may access these technologies for personal uses if the following restrictions are followed:

1. The use is lawful under federal or state law.
2. The use is not prohibited by Board of Governors, University or institutional policies.
3. The use does not overload the University computer equipment or systems, or otherwise harm or negatively impact the system's performance i.e. excess use of computing resources as in multiple copies of printouts, email-chain letters, personal 'announcements', general advertisement postings, etc.
4. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).
5. The use does not violate federal or state laws or University policies on copyright and trademark.
6. The use does not state or imply University sponsorship or endorsement.
7. The use does not violate state or federal laws or University policies against race or sex discrimination, including sexual harassment.
8. 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.
9. The use, when performed for non-work related activity, does not conflict with regular work assignments and does not represent more than incidental use for non-faculty employees.
10. The use of campus labs does not violate the rules and regulations set forth by the individual lab coordinators and departmental policies.
11. The use does not conflict with appropriate standards of civility and common courtesy or respect for the rights and privacy of others. Access to computing resources is a privilege that is granted on the presumption that every member of the University community will act responsibly. The University endorses the following statement on software and intellectual rights distributed by EDUCOM, the non-profit consortium of colleges and universities committed to the use and management of information technology in higher education and ADAPSO, the computer software and services industry association.

    a. "Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principal applies to work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy and right to determine the form, manner and terms of publication and distribution.

b. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

IV. Other Computer Usage Guidelines

A. Users are to have valid authorized accounts and may only use those computer resources, which are specifically authorized. Users are responsible for taking reasonable precautions to safeguard their own computer account. Users should treat computing resources and electronic information as a valuable University resource.

Users who publish home pages on the World Wide Web must identify themselves as the author. In addition, they must include the disclaimer that follows, or a similar disclaimer stating that any personal home page content reflects their own views and not necessarily that of the University. This disclaimer must appear on the main page and any subsequent page where the users (author's) name appears on the users web site.

> East Carolina University is not responsible for either the contents of this web page or any other page that can be linked from this web page and that the material is not endorsed, sponsored or provided by or on behalf of the University

In addition, any links to other web resources must be clearly identified.

B. Users may not change, copy, delete, read or otherwise access files or software owned by other parties without permission of the custodian of the files or the system administrator. Users may not bypass accounting or security mechanisms to circumvent data protection schemes. Users may not attempt to modify software except when intended to be user customized.

C. Users shall assume that any software they did not create is copyrighted. They may neither distribute copyrighted proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.

D. Employees must not use the computer systems to violate any rules in the East Carolina University Business Manual, North Carolina State Personnel

Manual, departmental rules, University policies or procedures, or any local, state or federal laws.

E. Students must not use the computer systems to violate any rules in the East Carolina University Student Code of Conduct, departmental rules, or any local, state or federal laws.

V. State and Federal Statutes

A. North Carolina statutes of which individual employees and students should be aware of that may bear on computer use include:

- 14-190-1, Obscene Literature and Exhibitions
- 14-456, Denial of Computer Services to an Authorized User
- 114-15.1 Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation.

B. Federal statutes of which individual employees and students should be aware of that may bear on computer use include:

- Title 18, Section 1030, Fraud and Related Activity in Connection with Computers.

VI. Violation of Policy by University Employees

A. Any violation of this policy is "misconduct" under EPA policies (EPA non-faculty) and "unacceptable personal conduct" under SPA policies.

B. Sanctions for violation of this policy may include one or more of the following: a revocation of access privileges; a written warning or written reprimand; demotion; suspension without pay; or dismissal.

C. Violations of law may also be referred for criminal or civil prosecution.

D. Violations of this policy should be reported immediately to:

1. The employee's unit administrator
2. Upon verification reported by the unit administrator to Employee Relations in the Department of Human Resources
3. In consideration of violation severity, Employee Relations will notify the University Attorney and the Chief Information Officer. (Upon notification, the Chief Information Officer may terminate computing resource access privileges pending investigation of the violation)

VII. 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 University records retention schedule and State Division of Archives regulations.

VIII. Violation of Policy by Students

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.

IX. Policy Questions

A. Employees' questions or concerns about this policy should be directed to the office of Employee Relations, Office of Human Resources.

B. Students' questions or concerns about this policy should be directed to the office of the Dean of Students, Student Life.

World Wide Web Policy

Purpose of Policy: This policy governs the use of the World Wide Web by ECU constituents

Person(s) with Primary Responsibility: CIO and Director of Strategic Initiatives

Approved: Chief Information Officer

Insofar as the university recognizes the value of the World Wide Web (WWW) as an effective information resource for all university constituents, including but not limited to current and prospective students, faculty, staff, alumni, and the general public for communication, education, research, and scholarship, it is further recognized that documents contained on it are a reflection on the creator(s) and the institution as a whole. Therefore, the content and appearance of documents and other subject matter contained on all web pages must comply with the following policies and guidelines.

Web Page Development:
All web page development must comply with the following university policies and guidelines:

1. Academic Computer Use Policy
2. University Student and Employee Computer Use Policy
3. Trademark and Logo Policy
4. Publications: Guidelines for Using the East Carolina University Logo
5. Patent and Copyright Policy
6. Advertising Policy
7. Policy Statement on commercial exploitation of classroom materials

Design Standards:
To achieve consistency at all institutional and unit levels, the web pages for any unit listed on the University organizational chart must follow the design standards established by the University Web Committee for the primary web page. Units are also encouraged to follow these same design standards for all subsequent web pages. It is strongly suggested that all web pages contain a date of last revision and clearly identify or be linked to a contact page that identifies the department, school, or individual responsible for the web site and identify the name, e-mail address, and postal address of the person to which questions and concerns on the web site should be directed.

Web pages containing content not related to conducting university business must provide the following disclaimer or a similar disclaimer on the main web page and any subsequent pages. All web pages located on the ECU "personal.ecu.edu" server will automatically display the following disclaimer at the bottom of each page without modification to the html in personal files.

> The content contained herein reflects the views of the author(s) and is not considered an endorsement by the university.

Access by Individuals with Disabilities:

In compliance with applicable state and federal laws, including Section 504 of the Rehabilitation Act, the Americans with Disabilities Act and university policies, university related, and university electronic publications must provide reasonable access to individuals with disabilities. Contact the Department for Disability Support Services for alternative methods in providing access to information contained on the site.

Oversight and Review by University Web Committee:

Oversight and review of university-associated policies and guidelines related to web pages is the responsibility of the University Web Committee. Monitoring of web pages located on the ECU network may occur to enforce university policies, state, and federal laws. The monitoring of web pages not related to the conducting of university business and housed on servers not under the direct administration of ITCS will be the responsibility of the server administrator. Violations of the web policy will be made known to the responsible unit administrator or Student Life representative for resolution. Non-compliance with University policies may result in removal of web pages and disciplinary action.

Appendix B - List of Internal ITCS Policies

GENERAL POLICIES

Code of Ethics
University Student and Employee Computer Use Policy
Academic Computer Use Policy
World Wide Web Policy
Advertising Policy
ECU Personal Digital Assistant (PDA) Support Policy
Open Mail Relay Policy

ORGANIZATION AND REPORTING STRUCTURE

Organizational Chart

PERSONNEL

Recruiting and Staff Development Policy
Promotion Policy
Hiring Policy
Criminal Background Check
Interview Policy & Procedures
New Employee Orientation
Separation Procedures
Compensatory Leave For Exempt Employees
Telephone Requirements For ITCS Employees

GENERAL ADMINISTRATION

Forms Control Policy
Long Distance Phone Usage
Control of Keys
Fixed Assets Inventory Control
Control of Hazardous Materials
University Owned Equipment Located Off-Campus
System Development Lifecycle
Change Management Procedure For Critical Level 1 Servers

CUSTOMER'S SERVICES

University And Non-University Accounts

DATA MANAGEMENT

Release Of Sensitive Information
Coordination With Internal Auditor
Software Development Programmer Access to University Production Data
Migration Of Software Programs To Production
Mail Purge Policy

SECURITY

Data Classification & Security
Security Of Data, Records And Hardware
Management Security Responsibilities
Spam Email Policy
Network Scanning Of Computing Systems
Security Incident Tracking
Database Security Violations
User Account Termination Policy
Supervisor Notification For User Account Termination
Antivirus Policy
Disk Sanitizing Policy
Password Expiration Policy
Workstation Security
ECU Departmental Server Policy
Bomb Threat Procedure
Physical Security In Computer Operations Areas

OPERATIONS

Production Scheduling
Special Run Request
Tape Library Procedures
Emergency Action Policy
Fire Fighting Procedures
Announcement Procedure For Proposed Downtime

Appendix C - IT Infrastructure

East Carolina University has an extensive information technology infrastructure that supports general needs, administrative systems, faculty, research needs and healthcare clinics. This appendix provides a brief description of the infrastructure available in each area.

IT Infrastructure – General Support

Campus Backbone and Network Description

The East Carolina University Fiber Infrastructure is divided into eight geographic regions, servicing the east and west campuses. Each of these geographic regions represents a fiber distribution point and corresponds to a fiber MDF (Main Distribution Frame). The typical fiber duct bank consists of three 4-inch PVC conduits, buried 30 inches below grade and encased in concrete.

The Campus Network Backbone is a meshed Gigabit switched Ethernet, using Gigabit routers in three key campus locations. Seven of the eight fiber MDFs are also electronic MDFs and use redundant links for network resiliency. (Electronic MDFs are fiber distribution points that also utilize electronic networking hardware to service surrounding buildings.) Network devices, links, throughput, etc., are monitored by the Network Operations Center (NOC) using advanced network management software.

The East Campus and West (Medical School) Campus are linked via a fiber optic link that spans over 3 miles and transmits data at 1 Gigabit per second. This fiber optic link was a result of a collaborative inter-local agreement between the City of Greenville, Greenville Utilities, Pitt County, Pitt County Memorial Hospital and East Carolina University. Each of these entities provided the capital needed to install fiber through key portions of the city in order to establish high-speed communications links, resulting in tremendous savings over the traditional telecommunications links typically utilized. East Carolina University previously utilized a 100-megabit microwave link for the East to West Campus data communications. This link currently is utilized as a redundant link for the fiber optic link.

The design of the campus network infrastructure meets or exceeds the baseline specifications set forth in the *UNC Network Assessment Minimum Network Specifications* **[17]**.

Computer Room Services and Hardware

The ITCS Operation Center provides academic and administrative computing services for the main campus and the Brody School of Medicine on a 24 hour x 7 day a week basis. The systems include an IBM Multiprise 3000 mainframe computer serving all administrative functions including the student system, the financial reporting system, payroll, financial aid, purchase orders, data warehousing and accounts payable of the university and an SGI Origin 2000 serving academic research services for the university. These computers are complex units with the mainframe computer-being a dual processor unit using the OS/390 operating system and the research system being a four-processor unit using the Unix operating system. The systems share communications, print facilities and tape storage devices utilizing an in house developed and maintained sharing scheme. Two Compaq Alpha servers using VMS services the Brody School of Medicine clinical patient scheduling, patient records and patient billing. Two IBM RS6000's are used for special applications and as WEB gateway servers. One hundred and sixty NT servers are used for departmental special applications, enterprise applications such as e-mail, distance education, student portals, staff and faculty portals, integrated voice response for student registration, departmental and student WEB pages and file and print sharing.

Peripheral input/output devices include five high speed impact printers, three medium speed duplex laser printers, IBM 3480 tape drives, Hitachi 7490E tape drives, IBM 3422 tape drives, DLTIII/IV/VII/O tape drives, high capacity robotic tape library for back-ups, IBM RAMAC 500gb mass storage device and more than 5 TB of server mass storage across all servers. Two NCS optical scanners provide automated test grading, grade posting and survey results. Bursters, decollators and folder/sealers are utilized for output processing.

Facilities include 7072 sq. ft. of controlled access and controlled environment computer room with raised flooring serviced by an Exide Model 3000 UPS system, a Halon Fire Suppression System and 60 tons of air handling equipment.

Help Desk and Student Help Desk

The University Help Desk: IT Support Services provides first-level phone support on a variety of IT-related issues to ECU faculty, staff and students. Basic responsibilities include resetting customer passwords, troubleshooting email accessibility, remote printing administration, and general application issues, static IP assignments, directing to various IT web resources and answering IT-related inquiries. Problems not resolved at this level are escalated to the next level of support.

Student Help Desk: The Student Help Desk provides first-level phone support on a variety of IT-related issues to the ECU student population, which includes on and off-campus, medical and distance education students. This help desk provides extended support outside the normal business hours of the University Help Desk from Sunday through Thursday, 4pm to 12am. Responsibilities include resetting email passwords, troubleshooting email accessibility issues, directing students to various IT web resources, and answering IT-related inquiries. In working with University Housing (REZNET), the Student Help Desk provides support to residence hall students experiencing problems connecting to the network.

Student Computer Labs

Student Computer labs are completely funded from the Technology Fee budget. ITCS chairs a Student Coordinator Committee to recommend configurations of hardware/software purchases and upgrades and to develop general operational policies and procedures. The lab coordinators will be working on various training sessions for new lab coordinators and lab assistants next year to improve the ability to provide students with the best possible service. The ITCS Lab Coordinator is ultimately responsible with working with the Director of ITC to coordinate the purchase and distribution of hardware, software, peripherals, and supplies to over 63 labs on campus. The ITCS lab coordinator is responsible for turning in the lab assistants' payroll and the distribution of checks for lab assistants from various labs.

Internet Connection to NCREN

NCREN (North Carolina Research and Education Network) provides Internet service to the East Carolina University campus network. The NCREN/Internet connection is currently an OC3 (155 megabits per second) ATM link **[18]**.

Data traffic utilization on the NCREN network is expected to increase 100 fold by 2006. In response to this expected growth MCNC, UNC-GA, and NCREN developed plans for the next generation network, NCREN3. This network plan calls for an upgrade to East Carolina University's campus connection to an OC12 (622 megabits per second) ATM link in October 2002. This campus connection provides communications with other NCREN constituents as well as the commodity Internet and Internet2.

Academic Library Services

Academic Library Services (ALS) is a branch of Academic Affairs and reports through the Vice Chancellor for Academic Affairs. ALS serves East Carolina University faculty, students, staff and visitors by offering library resources and services to support the research, instruction and service goals of the University. Academic Library Services consists of Joyner Library and its Music Library branch located in the Fletcher Music Building.

The Joyner Library Systems Department provides support for operations, services and programs of Academic Library Services by developing, enhancing and maintaining the information technology resources for the Joyner and Music Libraries. These IT resources include: online Library catalog system, Interlibrary Loan lending software, numerous databases and search engines, proxy software that allows off campus users to access electronic resources, academic video production and support, teleconferencing, and technology training.

William E. Laupus Health Sciences Library

The Health Sciences Library (HSL) serves as the primary information resource center for the University's instructional, research, and patient care programs in the health sciences. It also serves as the comprehensive information resource center for health care professionals who practice in northeastern North Carolina. In addition, the Health Sciences Library serves as a secondary resource for non-technical health care information for health care consumers in the local community. The Health Sciences Library emphasizes proactive information provision including the acquisition of current and relevant materials, reference services that recognize the existence of diverse levels of client expertise and needs, and the implementation of new technologies for accessing and managing information.

The Health Sciences Library Systems Department is responsible for all computing and networking technologies within the library including training, teleconferencing, operations support, server and workstation maintenance, customer support, maintaining the computer lab and classroom, and the HSL web presence. The Systems Department occupies two areas on the second floor of the HSL. One area houses the offices and hub room. The second area houses our Computer Lab and Computer Classroom. The Computer Lab is the only computer lab in the Brody School of Medicine and is the second largest computer lab on the ECU campus. The computer lab contains state of the art technology including 77 PCs, 10 Macs, 3 Flatbed Scanners, an Infrared Printer, and 3 networked HP Laser Printers. The lab provides a full range of computer services to ECU faculty, staff, and students. The software collection offers over 50 software titles in a variety of subject areas to compliment the Brody School of Medicine and the Division of Health Sciences curricula as well as word processing, spreadsheets, telecommunications programs, an extensive collection of medical software, and computer-assisted instruction programs for general use by all ECU faculty, staff, and students. All computers can connect to the Internet and provide users with access to electronic resources.

The computer classroom is located within the computer lab. This classroom supports the library's instructional services program and is also available for use by the Division of Health Sciences faculty, and staff. The classroom is equipped with 17 student computers, an instructor computer, a networked printer and a projection system to assist with software demonstrations. The classroom is also connected to the university's satellite broadcast network and is equipped for viewing video teleconferences.

OneStop Portal

Developed by ITCS Software Development Services, the "ECU OneStop" was placed into production on August 24, 2001. It offers a secure customizable portal environment that provides students, prospective students, faculty and staff with a single point of contact for user-specific information, applications and communications tools. Also, it allows rapid development and deployment of new applications with a focus on emerging technologies such as cell phone and Palm access. The ECU OneStop allows complete customer-centered customization - even the color scheme of the individual's portal - and has even been designed to allow channels of information to be easily added, removed, minimized, detached and rearranged to the user's satisfaction.

The ECU OneStop is the result of nearly three years of input from students, campus departments, staff and faculty. The majority of the past two years have been dedicated toward the development of this portal as a result of that input. ECU is proud to have been the first UNC institution to implement a state-of-the-art portal.

University Web Page

In January 1994, our first university web site, WWW.ECU.EDU, was launched online. Through the years, several web redesigns have been accomplished. The current ECU Home Page is the fifth redesign in the web site redesign series when it was placed online in March 2000. Throughout the evolution of the ECU Home Page, efforts have been continuously made to create a more seamless environment with a consistent navigation design interface running throughout the web site. Several templates have been made available for departmental use and technical help supporting unit adoption of the web templates is available through ITCS Strategic Initiatives. Strategic Initiatives continues to work with campus departments to redesign their sites within the parameters established through the latest web design initiative. As a result, the ECU Home Page provides valuable recognition and visibility for the University in addition to providing essential information to all university constituents from admissions information to ECU Pirate game stats and gift giving opportunities.

Wireless Connectivity

East Carolina University's wireless network consists of over 60 wireless access points located across both the East and West Campuses. Each access point uses 11 Mbs (megabits per second) shared network technology, supports up to 20,000 wireless workstation connections, and is connected to the campus network backbone. The ECU wireless network provides mobile network access to students, faculty, and staff in selected classrooms, libraries, dinning centers, and campus public areas [19].

IT Infrastructure – Administrative Support

Administrative Applications

ITCS Software Development Services supports a variety of application systems on varied operating system platforms:

Business Services/Financial System:

Accounts Payable/Receivable
Athletic Concessions
Budgeting
Campus Post Office
Central Motor Pool
Central Receiving/Stores
Demurrage (gas cylinder inventory)
Fixed Asset Accounting
General Ledger
Mail Services
Materials Management
One-Card
Parking & Transportation Services
Police Department
Printing & Graphics
Purchasing
State Reporting
Student Loan
Student Stores
University Mail Services

Marketing

SCT e~print

Data Base Administration:

- Computer Associates IDMS database
- IBM DB2 relational database
- IBM DB2/UDB
- Microsoft SQL Server database
- Oracle relational database

Distributed Application Development:

- Administration & Finance Web-Based Budget Report
- Brody School of Medicine (BSOM) Admissions (AMCAS/AWS)
- BSOM Business Affairs' Web-based Budgeting System
- BSOM Institutional Review Board Application & Review System
- BSOM Mobile Unit Tracking System
- Clinical Information Data Warehousing Analysis
- Departmental-base distributed applications/systems
- FoxPro/dBase IV applications conversion to MS-Access (and subsequent support)
- PDA-based Alumni Prospects Application (hand-held devices)

Human Resources

Applicant Tracking
Job Vacancies
Labor Distribution
Payroll
Personnel
Position Management
Telephone Directory
Check Reconciliation

IDX

Patient Appointment Scheduling & Physician Billing Modules:

- AES (Application Enhancement System) development system
- BAR (Billing & Reimbursement)
- DBMS (with a report writer)
- SCHED (Scheduling patients)
- MTRACK (Medical Record Chart Tracking)
- EFG (Encounter Form Generator)
- PCS (Paperless Collection System)
- SEC (Security Plus)

E-Commerce for patient claims filing

The following modules associated with a recently approved upgrade to IDX requiring additional action by the IDX team include:

- Ambulatory Visit Management (AVM)
- MPI-Link (Master Patient Index)
- Enterprise Wide Scheduling (EWS)
- Web 2.0/IDX release 9.0

New Technology and Development Group (NTDG)
The NTDG team is mainly responsible for information systems for the following areas:

- e-business/e-services applications (including web-enabling of administrative forms)
- e-commerce (credit card, debit card transactions)
- Kiosk/Cyber Café Units
- Portal infrastructure and applications (ECU OneStop)
- Student/faculty/staff Internet applications
- Investigation of new technologies relative to ITCS, SDS and its mission

Student Systems
The Student Systems team is responsible for information systems for the following areas:

Financial & Student Support:
Business Office
Cashier's Office
Cashier's Receipt
Counseling Services
Dining Services
Disability Support Services
Financial Aid
OneCard Office
Parking & Traffic Services
Sorority/Fraternity Affairs
Student Life

Enrollment Services:
Academic Affairs
Admissions
Degree Audit
Division of Continuing Studies
Graduate Studies
Planning & Institutional Research
Registrar's Office
Schedule25/Model25/Resource25
Student Housing
Undergraduate Studies

Financial Data Warehouse
East Carolina University's Financial System is a purchased package called Financial Reporting System (FRS) from Systems and Computer Technology Corporation (SCT). The underlying (non-relational) database is a product from Computer Associates known as IDMS. Functional end-users are neither able to directly access their data in real-time mode with IDMS nor are they allowed to access mission-critical production data files directly. The solution to providing end-users "point-and-click" access to their data is through a data warehouse utilizing a relational data base platform.

Data is extracted from the SCT FRS IDMS files on the IBM mainframe processor and loaded into a series of logically related tables (files) on IBM's relational DB2 database residing on ECU's IBM OS/390 mainframe processor. End-users are currently using MS-Excel and/or Brio-Query to access data directly from this data warehouse. A major advantage noted is that end-users no longer need to wait for an applications programmer to create their report(s) thereby reducing the time from hours and perhaps several days based upon workload, to just several minutes.

IT Infrastructure – Faculty Support

Faculty Workstation Program

ITCS is responsible for working with administrators in Academic Affairs (AA) to facilitate the refresh of faculty computers. Typically faculty or AA administrators provide input into a configuration that will meet the faculty's needs. A system based on those specifications is configured and ITCS works with vendors to obtain the best possible pricing. To conserve labor, keep installation costs down and to ensure standards ITCS creates a 'master disk image' of the selected machine for pre-installation by the vendor. Due to the purchase volumes, ITCS also facilitates the coordination of acquiring vendors to setup the new systems as well as oversee the technical and administrative management of the rollout project.

Faculty Instructional Support – Academic Affairs IT Consultants

The University hired 11 Instructional Technology Consultants (ITC), and assigned them directly to individual academic units. From the ITC website **[20]**:

> The role of the ITCs is to promote, support, and integrate digital technologies into learning and teaching at East Carolina University.
>
> A primary goal of the ITCs is to empower faculty members in the use of technology in education. They are available for consultation on course or project design, and are active in the implementation of technology-supported educational initiatives. They provide faculty with training by offering one-on-one tutoring, by designing and conducting group workshops and seminars, by preparing training materials that are made available either in print or electronically, and by making educational presentations at university or state conferences.
>
> The ITCs provide the following services to faculty members:
>
> - Consultation and planning for course design and delivery
> - One-on-one training for faculty in use of software and hardware
> - Group workshops within the unit on course design and implementation and/or use of software and hardware
> - Printed and on-line technical information and training materials for faculty
> - Campus-wide workshops that focus on developing strategies for transferring course content to an on-line environment, using the courseware Blackboard and other tools
> - Educational presentations and demonstrations at technology fairs, conferences, and workshops
> - Liaison with other campus entities, e.g., University Multimedia Center
> - Project organization and support

- Instruction on use of specialized equipment and software, e.g., digital cameras, Flash
- Research and recommendations on equipment and software needed for specific projects
- Research and provide information on copyright and intellectual property issues in technology and education
- Providing information on current technologies and their use in education to faculty and administrators
- Assistance in development of grant proposals for course projects using new technologies
- Facilitator for communications between faculty and campus technology support personnel
- Support for and dissemination of information about ECU's campus technology initiatives
- Service on intra- and inter-unit committees, ITC committee, and campus wide committees
- Participation on interdisciplinary project planning committees and projects

Blackboard Services

ITCS worked with the IT Consultants (ITC) to develop and offer Beginning, Intermediate, and Advanced Blackboard classes, as well as web-based tutorials for reference materials to the ECU faculty. These classes were offered on both main campus and the School of Medicine campus. ITCS provided assistance with the testing of new versions of Blackboard and consulted faculty on new upgrade features. Complimenting the assistance of ITCS, the departmental ITCs provide one-on-one assistance to faculty who are developing web-based courses.

BSOM Student Computing Requirement For Laptops and PDAs

In 2000 the Brody School of Medicine established the Student Technology Task Force to study the need and possible requirement for M1 (Medical, 1st year) students to purchase laptop computers and M2 and M3 students to purchase PDAs (Personal Digital Assistants).

In addition, two laptops were purchased with Student Technology Funds to assist students, whose personal computers failed, so they could continue their studies and complete their assignments on time. The information gathered from the BSOM Task Force later proved useful to the east campus Student Computer Task Force in performing a similar study.

University Multimedia Center

The University Multimedia Center (UMC) **[21]** is a graphic-design consulting group that works with the Academic Affairs Instructional Technology Consultants (ITC) and directly with faculty members to:

> *Enhance multimedia course offerings both on-and-off-line. In a collaborative effort with faculty who provide content expertise, and academic unit instructional*

> *technology consultants, the center staff applies the educational and instructional technology needed to make on-line courses high quality, effective for learning, and innovative. This resource facility will design and develop curriculum-based multimedia content as well as train/mentor interested faculty and instructional technology consultants.*
>
> *The UMC is an e-Learning resource for Distributed Education and Academic Information Technology (DEAIT) within Academic Affairs.*

Opscan Grading

The ITCS Operations Center offers Optical Scanning services (Opscan) to faculty members for grading student tests on standardized "bubble" sheets. The service provides the faculty with a hardcopy or electronic report of the student grades, usually within two hours. The Opscan service is also used for tabulating surveys.

IT Infrastructure – Research Support

CIITR (RAVE Laboratory)

The Center for Interdisciplinary Instructional Technology Research (CIITR) was established to provide leadership at the University for advancing and applying instructional technology research with the purpose of improving student learning. From the CIITR website [22]:

> *CIITR will recruit and support interdisciplinary instructional technology projects across campus and bring progressive instructional technology innovators together to exchange ideas, look for synergy among different campus-wide projects, and create next generation projects to sustain the momentum of new research. In exchange, CIITR will assist in publicizing and disseminating the state-of-the-art contributions of each project for maximal benefit to the ECU community. Not only will principal investigators and existing projects be given the opportunity to affiliate with CIITR, but individual faculty members who are interested in instructional technology research issues can also join the center and share in the creation of new research initiatives. As new research initiatives are created, they will be housed in their originating department for administrative oversight and research credit, but affiliated with CIITR to build cross-campus synergy.*
>
> *Thus CIITR's role is to foster, encourage and enable new research initiatives utilizing the strengths of ECU's faculty and staff. The permanent CIITR staff will be the catalyst for establishing a research agenda, in cooperation with the affiliated departments, schools and faculty members, and organizing the funding efforts necessary to implement this agenda.*

One of the more prominent CIITR projects is that of the Reconfigurable Advanced Visualization Environment (RAVE) system, the first of its kind in North Carolina

[23]. The RAVE system is a visualization tool that offers students, faculty and staffs an unprecedented opportunity for the construction and use of virtual prototypes and the viewing of complex graphical data in unique ways. From the RAVE website:

> *This advanced technology permits the creation, display, expression and exploration of large complex detests as a shared experience through a collaborative, interactive three-dimensional visualization environment. Visualization tools take advantage of human perception as a method for analysis and enable people to easily make sense out of what otherwise would just be a set of meaningless numbers by using the one third of their brain devoted to visual processing. These tools used the combined power of the human eye and brain to discern relationships by presenting complex data as multidimensional color images and animation. Above and beyond any other aspect of the learning process, visualization lies at the heart of understanding. It is through the use of an ever-increasing collection of media styles that we are able to represent better to students what, otherwise, would be vague concepts.*

Research Support (Healthcare Data Warehouse)

East Carolina University Division of Health Sciences is a nationally recognized leader in primary care medicine and maintains progressive programs in nursing and allied health sciences. The proposed Medical Database Development Program (MDDP) project will leverage the technological advances of the Brody School of Medicine electronic medical record systems to build a unique data warehouse for teaching and research purposes. The MDDP will enable researchers and administrators to understand the region's health care by analyzing the wealth of health information that is collected by the Brody School of Medicine administrative systems. Regional health data from the National Center for Health Statistics will be used to enhance the MDDP knowledge base. Initial development of data marts in specific areas, including preventive medicine and disease management will be created. In addition, the MDDP will be used to develop a Patient Origin Analysis (POA) system to track patients. The POA will focus on visually tracking and understanding how patients travel through their healthcare system.

The proposed program is consistent with the UNC's strategic priority entitled "*Creation and Transfer of Knowledge: Expand the frontiers of knowledge through scholarship and research and stimulate economic development in North Carolina through basic and applied research, technology transfer, and public service activities.*" Specifically, this project will establish an invaluable consolidated database, which facilitates the optimal use of information currently being collected. This database will be available to faculty in the Division of Health Sciences, with appropriate safeguards and guidelines for use. It is anticipated that this database will be utilized by faculty throughout the Division as well as by the ECU Center for Health Services Research and Development to answer a series of hypotheses related to health services utilization, health system practices, provider behaviors, preventive health interventions, and other related issues. The new knowledge derived from the database will enrich our teaching of learners in the health sciences as well as improve patient care practices at ECU and at similar health systems across the nation.

Project Purpose/Goals
The purpose of the proposed project is to create a unique and powerful database of health care delivery information that is appropriately encrypted and stored on a secure Intranet to insure patient confidentiality. To develop the proposed process that will extract information from the current system and build the MDDP, the following will occur:

- Construct a common data warehouse containing a ten-year history of relevant health information from both the ECU electronic medical records system and the ECU electronic patient billing system in which individuals are linked by a common numerical identifier. In addition, obtain similar national data from the National Center for Health Statistics for comparison to our regional data.
- Initially construct data marts for each of the following research and teaching areas: 1) chronic disease management (for example patients with diabetes mellitus) 2) preventive health measures performed to increase healthy lifespan (for example mammography) 3) pregnant women and their offspring to assess critical issues in maternal and child health, (for example the need for Cesarean section or immunizations in infants).
- Develop a user-friendly web interface that will enable faculty to easily query the data warehouse or data mart and produce output, which can be downloaded for further analysis.
- Develop a Patient Origin Analysis (POA) system, utilizing advanced mapping and graphics systems.
- Establish a system of encryption and security, which insures patient confidentiality.
- Establish an advisory committee of clinicians. The advisory committee will be charged with defining and prioritizing common domains of faculty research and interest, as well as reviewing and assessing the quality and completeness of all resulting data.
- Pilot test the database and insure confidentiality.

IT Infrastructure – Healthcare Clinical Support

IDX

IDX is a packaged software system for Physician Billing and Appointment Scheduling. There are approximately 150,000 active patient master records and a grand total of 553,773 active and inactive patient records stored on IDX. The system processes ~$108 million in charges and ~$60 million in receipts. Approximately 3,000 new patients are registered on the system each month.

The ITCS IDX Applications Group is responsible for providing application support services for the Brody School of Medicine and other integrated organizations associated with ECU. These application support services include the support of several applications.

The ITCS Systems Group provides system support for the primary production system and the test production system. This group provides 24-hour daily support and performance monitoring for the hardware (AlphaServer ES-40) and OpenVMS operating system; ISM or Mumps application layer support; database management; ensuring system security, monitoring interfaces between Logician and UHS; and implements new applications installations and upgrade projects. They also provide assistance to Operations, Production Control, and the Workstation group as needed for complex trouble-shooting needs.

Logician

Logician is the Electronic Medical Record (EMR) for Brody School of Medicine's outpatient clinics. The application is used at the point of care via desktop workstations or thin terminals and contains the patients' medical history including problems, medications, lab test results, and the providers' clinical notes. It also offers an extensive knowledgebase (drug interaction checks, patient education forms, reference articles, etc.) that support a patient's clinical encounter with School of Medicine providers.

- Oracle database (with 266,381 patient records as of 5/12/2002)
- Approximately 1150 clients
- Over 500-600 workstations (including Faculty Office's)
- Wireless Notebooks and Pen pads
- Real-time and batch interfaces to various external clinical systems (i.e. PCMH labs)
- Development of new technologies (Citrix server (described below) w/thin clients and/or wireless devices)
- Partnership with School of Medicine Telemedicine program

The ITCS Systems Group supports the primary Logician server and the additional servers associated with Logician. There is a Logician fail-over system (Logician2), medical image server, and transcription server. This group assists in the 24-hour daily support and performance monitoring, ensuring system security, monitoring of interfaces, expansions of on-site and remote clinical areas, and testing of development technologies. They also provide assistance to Operations, Production Control, and the Workstation Support Group as needed for complex trouble-shooting needs.

Citrix

Citrix Thin Client technology allows physicians remote access to business-critical applications such as Logician and IDX over the network or Internet. This technology assists in delivering the applications without having to load the full-client package enabling faster upgrades and rollouts in a centralized manner. Citrix requires NT authentication and provides an additional layer of 128-bit security encryption.

The ITCS Systems Group provides the Windows 2000 Advanced Server support, hardware support for (3) Citrix Servers (1) NFuse Server, (1) Packaging Server, and (1) Test Server, and Citrix Metaframe support. This group trains the Workstation group on how to support this environment and is the same staff supporting Logician.

Consolidation of Brody School of Medicine Informatics and CIS

In October 1999, ECU Computing and Information Systems (CIS) and the Brody School of Medicine (BSOM) computer department consolidated to form the Information Technology and Computer Services (ITCS) Division. ITCS is responsible for administering and maintaining information technology for the University and the BSOM.

In the 4th Quarter 2002 the ECU East Campus Operations Center and the BSOM West Campus Operations Center will be combined into a single operations center. This consolidation coincides with the relocation of ITCS to a new computing facility, which will employ new physical security measures not available in the current facility structures.

Appendix D – SDLC Form

This is an abbreviated SDLC form used for the initial review of an IT initiative.

Systems Development Life Cycle Summary Form

(This is a Word Form. Move from one entry field to the next by pressing the Tab key. As long as you type continuously, the lines will wrap at the ends. If you want multiple paragraphs under a heading, you may press the Enter key as long as there is at least one space between your cursor and the end of the gray text field.)

Note: If this is a clinically-related system, it must first be reviewed by the Clinical Information Systems Steering Committee Chair.

Describe the system and hardware being requested:

What administrative functional process(es) does this impact? (Student, Financial, Human Resources, Facilities, Patient Care, Development, Sponsored Programs, Other)

Describe the purpose of the system and hardware being requested (i.e. Enhancement to service, to meet external requirements, etc.

Are there any efficiencies being gained? Yes □ No □
If "Yes", please describe:

What technical resources are needed for implementation? (Staff/Equipment, include salaries if new staff are needed.)

What functional resources are needed for implementation? (Staff/Equipment)

What is the amount of funding needed and what is the source of that funding?

Are there space and or facility requirements for implementation? Yes □ No □
If "Yes" please describe:

System Maintenance

What Technical resources are necessary for maintenance of the system and hardware being requested? (Staff, Equipment, Space)

What functional resources are necessary for maintenance of the system and hardware being requested (Staff, Equipment, Space)?

What is the estimated funding required for maintenance of the system (Annual Maintenance Contracts, etc.)? What is the source of this funding?

Who are the customers of this system and related processes?

Will training be needed for customers? Yes □ No □ If "Yes", who will provide training?

Are there any University policies or procedures that need to be updated or changed related to the implementation of this system? Yes □ No □ (If yes, please explain and indicate who will make the changes)

What are the consequences to the University if the implementation of this project is unsuccessful?

Submitted by: __

Signature:

Date: