BOSSIER PARISH COMMUNITY COLLEGE

POLICIES AND PROCEDURES

COMPUTER SERVICES

REVISED April 22, 2016

Approval:

Gary Hollatz
Chief Information Officer

Tom Williams
Vice Chancellor

Electronic Data Systems Policies and Standards

Bossier Parish Community College

Table of Contents

Electronic Data Systems Policies and Standards

Bossier Parish Community College

1.0 **Scope, Purpose, and Accountability**

1.1 **Scope**

The standards and policies presented herein govern data systems, infrastructure and usage at Bossier Parish Community College. These standards and policies apply to all computerized systems and associated information technologies involved with the creation, updating, processing, outputting, distribution, and other uses of electronic information at Bossier Parish Community College. They are extracted in part from common standards at educational institutions throughout the United States, and reflect standards for security and auditability. All specifications indicated are independent of system architecture and apply to mainframe database systems, networks of microcomputers, stand-alone microcomputers, and any other information technology whether developed at BPCC or acquired from external vendors. The standards apply to all applications that deal with financial, academic, administrative, or other electronic data systems at Bossier Parish Community College of Louisiana. The policies contained herein will be reviewed periodically and supplements/changes made as needed. The College community will be notified of such changes per the distribution procedures outlined herein.

1.2 **Purpose**

The primary purpose of these standards and policies is to establish system ownership responsibility and to ensure that each data system meets functional requirements, is appropriately documented, is secure and controlled, has been adequately tested, is maintainable and provides audit features.

1.3 **Accountability**

The owner of an administrative system defines the scope of a data processing project, develops an implementation and maintenance plan, assigns all associated responsibilities, manages the project, and is accountable for its operation and results. (An administrative system owner who does not use the services of the Computer Services for the design, development, or maintenance of an administrative system must assume both system ownership and the system developer responsibilities.) Operators of distributed data processing systems, remote network nodes, or small stand alone systems must satisfy all the responsibilities of system owner, system developer, and operator. **The College Computer Services shall have final authority over all data processing systems,**

information technologies, and networks associated with BPCC, including the authority to access, evaluate, and/or suspend the operation of a data processing system or network associated with Bossier Parish Community College of Louisiana.

1.3.1 System Owner Responsibilities

1. Define the functions, controls, manual office procedures, and auditability features of the system.
2. Ensure that the appropriate hardware and software is selected for the system.
3. Ensure that adequate controls, audit trails, security backup, recovery and restart procedures are included in the system design.
4. Ensure that the system is auditable.
5. Ensure that there is an adequate plan to test the system without loss or corruption of data.
6. Monitor system testing and review of the system during development and periodic maintenance.
7. Ensure that the design and coding of the system meet all appropriate standards.
8. Provide for the completeness and accuracy of all required documentation for the system.
9. Define and ensure compliance with the system acceptance criteria.
10. Formally accept the system as complete and ready for installation.
11. Define and ensure compliance with the system installation procedure.
12. Define and monitor procedures for modifying the system.
13. Authorize and document all hardware, software, and functional changes to a system.
14. Manage, control and review access to data.
15. Maintain and review data security and integrity.
16. Define and manage data sharing procedures in order to ensure the integrity of interfacing systems.
17. Designate a system operator or administrator responsible for day to day decisions regarding the operation of the system.

1.3.2 System Developer Responsibilities

1. Develop the defined application to the satisfaction of the system owner.
2. Translate the system functions into design and functionality requirements.
3. Design, code and test the application in compliance with all appropriate standards.
4. Implement the most effective methods of satisfying the control and auditability requirements established by the system owner, or resulting from design decisions.

1.3.3 System User Responsibilities

1. Comply with security requirements as established in College and state EDP policies

2. Comply with all control requirements specified by the system owner.

1.3.4 System Operator Responsibilities

1. Create and maintain a secure data processing environment that promotes efficient use of the data processing system.

2. Ensure proper operational environment with regards to environmental elements. (i.e. moisture, dust, power fluctuations, vibration, etc.)

2.0 Development, Review, Installation, and Modification of Electronic Data Processing Systems

2.1 Application Environments

Microcomputers: Microcomputer applications used for financial, administrative, academic or other ongoing business related purposes must comply with all appropriate administrative computing standards. These standards apply whenever the job functions of one or more individuals would be affected by sudden failure of the microcomputer application.

External Systems: Systems supplied by external vendors must comply with all appropriate administrative computing system standards. External system acquisition imposes the following special responsibilities on the system owner; proposing selection criteria; contacting potential vendors, securing approval of system design, and for acquisition from the Technical Review Committee.

Batch Systems: Batch systems must comply with all appropriate administrative computing standards when the system deals with financial, administrative, or other business information that is integral to the operation of the College.

Database Systems: As of July 1, 2011 the LCTCS adopted a multi-entity version of Ellucian’s Banner series of software for use by member institutions. Thus, Ellucians’s database packages are the standard for administrative processing at BPCC and adhere to the following database systems environmental criteria:

To minimize personnel retraining when employees change jobs, change job functions, or to assist other

offices during pervasive use periods, such as registration, a standardized user interface will be implemented for all administrative systems.

Procedures for rigorous documentation, monitoring, and program control of update transactions, should be in place for all administrative systems. Such strict control implies the use of full screen programs for maintenance activities, however line-by-line updating may be considered for less critical maintenance activities.

2.2 **Base Program Modification**

Building, installing, modifying, or upgrading data systems require significant expenditures of resources (people, computer time, etc.), therefore they must first have direct approval of the Director of the Computer Services. **Under no circumstances should a programmer or any College personnel install or in anyway modify a base program without the written approval of the Computer Services Director. Modifications of external systems shall be documented by the system owner and information regarding the change and impact shall be disseminated by BPCC Computer Services.**

A base program can not be modified, or installed without the approval of an ad hoc review committee convened by the Computer Services Director. The committee shall include the Computer Services Director or designee, the custodian(s) of the effected data, system security interests, the senior programmer, the requesting agent or representative, and any other individuals who may be affected by the action

3.0 **Administrative Programming Services**

Administrative programming services are provided to the College community by the Computer Services programming staff. These services include, but are not limited to, systems analysis, design, programming, implementation, database queries, and selected training.

3.1 **Request for Programming Services**

Request to the Computer Services for programming services fall under three categories - new programs, changes to existing programs, implementation of existing programs. A request for programming services will normally be initiated by the user and must be in writing.

The user should complete a request in writing. Requests for programming services require the following information:

Name, telephone #, and e-mail address of the person of whom questions and/or output should be directed.

1. Requested completion date. (A minimum of two working days is required)
2. Description of the request.
3. For access to or release of secure information the signature of the data custodian or designee is required. The three primary data systems and associated custodians are as follows:

Student Information System
(SIS) College Registrar

Financial Records System
(FRS) College Business
Affairs

Human Records System
(HRS) College Business
Affairs

3.2.1 Review of Programming Request

All requests for programming services will be made in writing and reviewed by the Computer Services Director or designee who will assign the program to the appropriate programming personnel. The request will be prioritized and the user notified if a change in the requested completion date is necessary. In most cases a "first in first out" approach will be taken.

Building, installing, modifying, or upgrading data systems require significant expenditures of resources (people, computer time, etc.), therefore they must first have direct approval of the Director of the Computer Services. **Under no circumstances should a programmer or any College personnel install or in anyway modify a base program without the written approval of the Computer Services Director.** (see section 2.2)

4.0 Programming Assignments

Under no circumstances will a programmer take on a program or project unless it has been approved and assigned by the Computer Services director. Only requests made in writing will be considered. The programming staff will not accept phone or verbal requests.

Programmers may be given individual assignments or assigned to a team to complete a project.

All programming assignments will be initiated using the written request.

It is the responsibility of the Computer Service director to review the Data Request to insure proper authorization of the requester before assigning the program task to a programmer.

4.1 Program Testing

The goals of testing are to eliminate errors from application functions before they are put into production; to ensure proper extraction of data; to begin user training and check documentation; to ensure that all interfaces disburse and receive data properly; to check utilization and cost of operation.

All new processing or base programs or programs that have been modified must be tested before being placed into production.

Tests will be made against data stored in test directories. **Production data will not be used to test modified or new programs.**

Programs, upgrades, or modifications will not be placed into production until they have been tested and signed off on by the Director. Where appropriate, the requester may also be asked to sign off on the program based on the test results. Base program modifications, installation, or upgrades require the approval of the Computer Services Director before they are placed into production.

Once the program is placed into the production mode it may only be modified by request of the user. Submission of a written request is required for all program modifications.

4.2 Procedure for Placing Programs into Production

Reserved for future use.

4.3 Procedure for Placing Programs on to the Production Calendar

Reserved for future use.

4.4 Program Naming Convention Policy

Reserved for future use.

4.5 Modification to Ellucian Banner Delivered System.

The Chief Information Officer and the Director of Computer Services will be collectively referred to as the “Director”.

While modifications to the Ellucian Banner delivered system should be kept to a minimum, it is understood that some changes are inevitable.

a. Changes must be submitted on the LCTCS Change Management Form which is available on the Comuter Services website.

b. The Director will evaluate the requests to assure that these changes are necessary and were requested by someone in authority. The LCTCS and its designee is the final authority for approval. Approvals must be obtained prior to implementation. The Director may use any resources available to decide or influence an approval or denial.

c. All source code will have the comments "*** BPCC...." immediately before and after changes to delineate modifications. In a case where there is no source to comment, e.g. screen change, a snapshot of the before and after screen will be submitted to the Director for insertion into hard copy modification binder.

d. Deviations from this policy are discouraged; however, the case may arise where this is required. Deviations will be submitted in writing, along with details and reasons for the deviation, for evaluation and approval by the Director. The Director has final approval authority.

e. Denial appeals must be submitted in written form to the Director's supervisor for arbitration. The Director's supervisor is the final authority in all matters arising from this policy unless the authority is reassigned to another person of equal or greater hierarchical ranking.

e. The Director will maintain records of all modifications. The records will include the following information:

a> Director or Division Head requesting change,
b> Description of modification,
c> Program(s), screens, library members, etc., affected,
d> Programmer making the change,
e> Date changes are to be implemented
f> Details of any deviations from this policy

4.6 SCT Time of Solution (TOS) Patches

Reserved for future use.

4.7 Formal Review and Installation

Reserved for future use.

5.0 Control, Security, and Auditability

The following establishes responsibilities and minimum requirements for the protection of Bossier Parish Community College data assets, and describes the necessary control, auditability, and functional features of computing systems necessary to maintain data security.

5.1 Responsibilities and Scope of Control

Control Responsibility: The system owner is responsible for the implementation and administration of all control and auditability functions of owner's data system.

Functional Control: System control procedures for the functionality of the system should include: initiating transactions; data descriptions and edits; processing transactions entry descriptions; communications methods; computer configurations; data storage and retrieval procedures; output processing procedures; output distribution; data recovery procedures; and data storage documentation.

Auditability Requirements: System auditability requirements will include; editing capabilities to ensure the integrity of input and output data; journalizing or logging to create a transaction audit trail for online systems; and verification/comparison checks to validate the accuracy and integrity of programs and data.

5.2

Data Access

Access authorization: The system owner authorizes/restricts access to data within a system.

Functional Access: Access to data will be provided only to those who need it to perform their respective functions. Access to some data sets or functions may be granted on an as need basis by the security officer. Request for such access is made in writing.

Data Sharing: Data will be shared among programmers with access needs in such a way as to minimize the duplication of databases and data elements.

System: Production system components must be kept in protected files with appropriate audit trails of all changes.

Damage Prevention: Data security must be designed to prevent both accidental as well as deliberate destruction or unauthorized alteration of data.

Sensitive Data: All files with sensitive data must be made secure against unauthorized access

5.3 **User Identification and Access Permission**

Access Restriction: Access to system applications will be controlled at logon and job initiation, based on verified user identification and authorization .

Restriction Scope: Access restrictions will apply to sensitive system resources such as commands, transactions or data.

Separate Directories: Development and test directories will be kept separate from production directories.

Password Standards: Passwords will be a minimum of 8 characters, changed frequently, and always changed on any accounts accessible by a former BPCC employee. Provision should be made for the non-display of passwords. Initial passwords will be pre-expired and will automatically expire after 45 days of existence.

Access Monitoring: Systems will be monitored for unauthorized access attempts, and will restrict repetitive attempts to gain access in order to forestall unauthorized entry.

Electronic Signature: A valid user name and password are required for access to a data system.

5.4 **System Interfaces**

Each point where data transfers from one system to another must be secure, and the transmission media must be protected from unauthorized access.

Data Custodian: The custodian of data being communicated determines format, content definition, and associated procedures. The data custodian is the College officer responsible for maintaining the official or enduring record of data being communicated.

Data Sender: The sender of data is responsible for the integrity of the data being sent. The data must be fully edited, accurate, and complete.

Data Backup: The sending system operator is responsible for backing up all system data according to a schedule approved by the system owner.

5.6 **Backup and Recovery from Interruptions**

Backup Files: All critical data files will be backed-up nightly to facilitate recovery in case of data loss. All source program files, faculty/staff, and student files must be backed up weekly. All backup files must be secured as originals.

Offsite Storage: At least one backup should be maintained offsite, for all essential applications.

Restoration of Data: In the event of data loss, files must be restored from the latest backup.

Recovery Process: A disaster recovery process should be in place for all essential systems in order to ensure the ability of the institution to survive business interruptions and to function adequately after an interruption.

5.7 **Security Administration Procedures**

The system owner must assign the responsibility for changing the rules and circumstances of authorization; for adding, changing or deleting users; and for changing specific user privileges relative to an administrative system.

System Journaling: All events taking place at the system/user interface should be journaled or otherwise recorded, in order to determine personal accountability. The system owner, security officer or designee maintains the Journal

Correcting Errors: System resource use, security variances, and delegation activity should be regularly monitored by the system owner to trigger timely and appropriate corrective action whenever necessary.

5.8 **Securing Hardware/Software**

All administrative system computing equipment, programs, files, logs and documents should be kept in physically secure areas in order to provide protection from unauthorized access and acts that would cause hardware or program malfunction.

When a workstation is surplused or transferred, it is the responsibility of the budget unit to ensure that there are no data on the hard drive that may be compromised. All files must be removed from the drive(s) before the computer is relocated or reassigned. In addition, licenses for software that remain installed on the computer must move with the computer.

5.9 Encryption of Transportable Media

All sensitive data that is stored on agency approved portable storage devices (Notebook PC's, USB thumb drives, USB hard drives, CD's, DVD's, diskettes, PDA's, etc.) that are removed from the state premises must be encrypted and consistent with OIT STD 023 Encryption Standard).

6.0 **Documentation**

6.1 **Development Process**

Documenting the process of developing a data system is the responsibility of the system owner. The development documentation should record the following information:

Personnel: A list of the personnel involved with the project, including the system owner, system developer, development team, and user test group.

System Requirements: The functional requirements as agreed to by the owner and developer, and the necessary data elements.

Design Plan: A plan for each iteration of the system, or of system components, including the testing and review process.

Test Plan: The system test plan, testing log and results.

Code Reviews: A log of all code reviews with results, reviewers and exceptions.

Systems Review: The formal system review results, reviewers and exceptions.

Modification: A description of the authorized modification process.

Formal Installation: Authorization for installation including: name of system; the system owner; the location of the productions system; file and table definitions, input and output screen and printer formats as well as source and object modules, and a list of all other systems that receive output from or provide input to the system.

General Design: A flow diagram of the program modules, files and subfiles.

System Interfaces: A description of all interfaces with any other systems, and specification of procedures and controls for assuring data security and integrity relative to the source system, the interface processing, and the receiving system.

File Structure: A list of names and files indicating where system/module code is stored.

Hidden Processing: A description of any major processing occurring inside a system which is not initiated by user actions.

Program Code: Commented code written to the standard.

Element List: A list of all database elements with full definitions, including the source of the data and editing precautions for ensuring the reasonableness of input and output.

Access Control: specifications of constraints on user access and a description of the modes of access restrictions.

Output Formats: A description of all screen and report formats .

Data Storage: A description of data storage and backup procedures.

Data Changes: Specifications of the user access journaling and description of any review and approval procedures relative to changed data.

Recovery Procedure: A description of the processes involved in restoring data and system integrity subsequent to a system failure.

6.2 **User Documentation**

User documentation is the responsibility of the system owner. The system developer is required to provide an on-screen help environment which is understandable, internally consistent, and easy to follow for both experienced and new user. User documentation should contain the following components as needed:

Welcome Screens: At the beginning of each separate operation a screen should identify the system/sub-system in use and describe its function.

Help Screens: The system should provide support information that is easily accessible, well organized and complete.

Error Messages: Users should be notified on the work screen when an error has occurred, and be prompted to correct the mistake.

Data Elements: A list of clearly defined data elements including input source and error checking process.

User Initiated Processes: A description of any major processes occurring within a system in response to user action.

Processing Screens: Illustrations of all entry and reporting screens with explanations of their uses, cross referenced to on screen help and instructions.

Reports: Standard reports produced by the system, frequency of automatically generated reports, calculated data fields in reports, and instructions for requesting user initiated reports.

Task Instructions: Specific sequential instructions for performing tasks that use the system or its component subsystems.

6.3 **Technical Systems Documentation**

Technical systems documentation is the responsibility of the system owner. The system administrator or other system users are required to provide any pertinent information related to system design, performance and functionality. This documentation should be easily accessible and understandable by both experienced and inexperienced users. Technical systems documentation should contain the following components as needed:

Personnel: A list of all personnel involved with the system. This includes, but is not limited to, the system owner, system developer, system administrator, development team, and user support group.

System Requirements: All functional requirements of the system as agreed to by the owner, developer, and administrator

General Design: General layout of the system. This may include flow charts, diagrams, and all other system design information.

Test Plan: A plan for testing the system without interruption of services to users.

Systems Review: System review results, reviewers, and exceptions.

Modification Plan: A plan for modification of the system. This should be done so that service is not interrupted to users.

Installation Guide: A guide for installing any new service, hardware, software or system.

Access Control: Specification of all constraints on user access and a description of all modes of access restrictions.

Backup Plan: A complete plan for backing up any aspect of the system.

Recovery Plan: A complete plan for restoring the system after a system failure.

System Journal: A complete log of all systems updates, modifications, or any other changes made to the system will be recorded.

6.4 **Software Documentation**

The Administrator is responsible for maintaining accurate documentation for all software on a given system. The information should be provided to the Director of the Computer Services and an additional copy located near system or one easily assessable from the system. The information documented should meet the following specifications:

- Describe functionality or purpose of software depicting any special installation notes or requirements.

- Document user base of provided software.

- Document vendor information including place of purchase, support contact information, and any personal technical contacts for the institution.

- Document version and/or revision of software release.

- Document license information and maintain any expiration information.

- Provide safe and organized storage of original media. All electronic-supplied software should be copied to an industry-standard medium and archived within license agreement accordance. Non-RAID fixed hard drive storage is not tolerable as an archive medium.

- All vendor-provided software documentation should be archived with original media copies. Copies should be in accordance with license agreement and should be stored near system and used for daily activities. No original documentation should be in direct possession of any operator without the existence of an archived original release.

- Report expiration information to the Director of the Computer Services in adequate time frame to consider substitutes, purchase constraints, or any information required for continuation of software service.

7.0 **Computer Software**

Any software loaded onto College computers must support College business. This includes software purchased by the College or by a College employee or student. The Computer Services staff may remove any software from a system that is not licensed, is deemed inappropriate or is in any way detrimental to hardware, software, or the College network.

7.1 **Licensing**

1. Regardless of ownership, all software running on College computers must be licensed.
2. Licensing documentation will be secured and available for review upon demand.
3. College technical or support personnel will not load or transfer licensed software without proof of license.
4. Computer Services may remove from a computer any software that is not licensed.

7.2 **Copying Of Computer Software**

Unlawful software copying is not permitted. Vice-Presidents, department heads, and directors are charged with ensuing that College faculty, staff and students are aware of and observe restrictions against unauthorized copying and use of computer software, as provided in the attached guidelines.

7.3 **Guidelines**

Scope of Policy: The prescription against unlawful software copying applies to all faculty, staff and students. The policy applies equally to all software computing devices.

Sanctions for Violation: Disciplinary steps will be taken against individuals violating this policy in the course of College related activities, or using College facilities to conduct or assist in unlawful copying, under the procedures appropriate to students, staff, or faculty as the case my be. For example, unlawful copying would be considered misconduct by members of the College staff, and in appropriately severe circumstances could result in discharge for cause.

Responsibility for Compliance:

- When software is acquired by the College, the using budget unit is responsible for reading and adhering to the terms of the license agreement and preventing unauthorized copying.

- When software is acquired by the College, the budget unit making the purchase is responsible for maintaining records necessary to show ownership of the software. (i.e. purchase orders, manuals, and original diskettes/CD's as provided by the software vendor.)

- Supervisors should ensure that employees and other persons having access to software are advised of restrictions and do not make copies without permission.

- Software purchased by individuals is the responsibility of the individual. Persons who knowingly aid in unauthorized copying also may be liable. (e.g., by loaning software to another person with the intent that the borrower will make an unauthorized copy, or by knowingly allowing one's computer to be used for making an unauthorized copy.)

Notification: Copies of this policy and these guidelines shall be made available through the college web page, in the college library, and upon request through the Chancellor's office and the Office of Student Affairs. Also, all Vice Presidents, Deans, and Department Heads will be provided a copy of the document. Supervisors are charged with ensuring that applicable employees are aware of this policy. Additionally, the following actions should be taken:

Self-service Microcomputers: All College self-service microcomputers (e.g., those in the libraries available for patron use) shall have on them, or nearby and visible to the user, a notice stating that unlawful copying is prohibited. The suggested form for such notice is : **NOTICE**: *Copying software or documentation may be subject to the Copyright Law. Unlawful copying is prohibited.*

Software: Lending Libraries- College software lending libraries shall undertake appropriate measures to ensure that patrons are advised that copying of the loaned software is prohibited (unless the software is in the public domain or the owner has consented to copying). Such steps shall include all or some of the following: signed statements by the borrowers, posted signs, labels on software and documentation, and warnings displayed on the computer screen.

Software Labels: Supervisors shall ensure that labels and notices prohibiting copying are not removed from software acquired by the College and that copies lawfully made include duplication of such labels and notices.

8.0 **Financial Accounting Systems**

The College has acquired many small computer systems used for a broad range of activities, including financial accounting. Some accounting information is now transmitted from these small computer systems directly into the primary accounting applications systems processed by the College's main computer. Standards and controls for the subsidiary systems are necessary to insure that the accuracy and security of the College's accounting information are not compromised.

8.1 **System Requirements**

Any computer system that originates or transforms financial data to be entered into the College accounting system must meet the following requirements:

> *Reconciliation with General Ledger*: Financial data to be entered into the College accounting system must be reconcilable to the College's General Ledger and must use appropriate account numbers (including expense and/or income classifications). The Controller's Office, Business Affairs, will review the system to ensure that these conditions are met.
>
> *Integrity of Data*: The system must possess effective security against accidental destruction and tampering, and sufficient audit trails and controls to satisfy standards set by College policy, government regulations, privacy laws, and generally accepted practices in the accounting and data processing profession.
>
> *Production Standards*: To insure that the College can make its monthly and annual closing deadlines, all systems integral to the accounting process must meet certain standards of reliability, documentation, and system back-up. Any feeder system that interfaces with the main College computer must meet these production standards.

9.0 **Computer Network and Telephone Usage Policy/Procedures**

Computing resources at Bossier Parish Community College are provided for the use of students, faculty and staff to help carry out the mission of the College. The College encourages and promotes uses of computing and network resources by the College community that support this mission.

Computer systems/electronic information systems include all computer based hardware, and software owned by the College, any communications hardware and software provided by the College for the purpose of accessing its computers, and any computer network governed in part or whole by the College.

Bossier Parish Community College generally provides users access to computer services such as electronic mail and the Internet twenty-four hours a day, seven days a week. (The College reserves the right to bring these services down for maintenance as needed.)

BPCC's Network is composed of two major segments.

1. Backbone
2. Subnet

A *Backbone* is defined as being any major link that connects multiple Subnets together. These Backbone segments are under the direct control of the BPCC Network Administrator. The Network Administrator sets and maintains all standards related to these connections to guarantee maximum network throughput and reliability. The standards include physical wiring and layout, along with protocols used to transmit data on the network. Any Subnet connected to a Backbone, that is causing network downtime or disruptions, will be disconnected from the Network Backbone.

A *Subnet* is defined as being any network placed in a given area or department that connects only a small number of computers. A Subnet is connected to the Backbone to gain connectivity to the rest of the College Network. These Subnets are under the supervision of the Network Administrator. In some cases, on large Subnets a person, from within a group or department has been given the responsibility of basic network troubleshooting. Any person such a position is not, however, authorized to approve network modifications or approve network hardware or software purchases. If there are any problems with the network backbone or changes that need to be made, the BPCC Network Administrator should be contacted immediately.

9.1 **BPCC Network**

9.1.1 **General Guidelines**

- The College Network is defined to include **<u>any</u>** and **<u>all</u>** computer-based communications facilities, which are owned or operated under the supervision of Bossier Parish Community College.

- The College Network is for use by authorized persons legitimately affiliated with BPCC, consistent with, and in the course of, their official work, study, and/or research.

- The BPCC Network Administrator must approve all physical connections/modifications to the College Network.

- The BPCC Network Administrator must approve any network hardware and software, before purchase. Any purchase requisition related to network hardware or software must first have the approval of the Network

Administrator or Director of the Computer Services before purchase can be made.

- To maintain network security, for all new network additions all hubs and switches must have built-in port security.

- Any wiring being installed by College personal or by a contractor must follow current wiring standards. The Network Administrator will over see all contract work on the network. Payment for such work will not be rendered until the Network Administrator approves the work.

- Computers with file sharing enabled may not connect to the network. Enabled file sharing presents a significant risk of unauthorized user access to secure data.

- The cost of network/phone wiring or equipment will be the responsibility of the associated budget unit.

9.1.2 **Network Usage Policies**

Individual groups or projects within BPCC may adopt more restrictive network usage policies that apply to their sub-networks and personnel within their area.

9.1.2.1 **Acceptable Uses:**

- Communication for professional development, to maintain current, or to collaborate in research and education.

- As a means for authorized users to have legitimate access to remote facilities.

- The publication of information via the Internet's World Wide Web (WWW), File Transfer Protocol (FTP), or similar techniques.

- Other administrative communications or activities in direct support of BPCC projects and missions.

- Individual groups or projects within BPCC may adopt more restrictive network usage policies that apply to their sub-networks and personnel within their area.

9.1.2.2 **Prohibited Uses include:**

- Use for personal or for-profit activities.

- Use by friends, family members, relatives, or others not officially affiliated with and authorized by the College. The BPCC network, including its dial-in lines, are not available as a substitute for private Internet service providers.

- Any use that is likely, or intended, to cause unauthorized Network disruption, system failure, or information loss.

- Any use related to achieving, enabling, or hiding unauthorized access to systems, software, or information either within or outside BPCC.

- Direct dial-up to a computer or network device connected to the College Network without going through the College modem bank.

- Direct connection to a College device via an outside Internet service provider (ISP).

- Bypassing or building a conduit through the College fire wall.

- Any use which violates BPCC EDP Administrative Policies.

9.1.3 Internet Use Policy

Bossier Parish Community College subscribes to its Internet Service Provider's Use Policy as follows:

> The use of College network facilities, including the BPCC network for Internet access, for any reason other then for College related activities, is strictly forbidden. Violators may lose access to College facilities and/or the College network and be subject to state or federal civil or criminal penalties.

9.1.4 LONI Use Policy

LONI exists for the primary purpose of transmitting and sharing information among governmental and educational organizations within Louisiana. Transmission of any material in violation of any federal or state laws or regulations is prohibited. LONI connections shall not be used to access other machines without the permission of the owner. The Subscriber agrees to observe the acceptable use policy of any other network the Subscriber accesses through LONI. LONI subscribers are expected to be responsible in their use of the network and avoid actions that cause interference to the network or cause interference with the work of others on the network.

9.1.4.1 LONI Use Policy for Internet Access:

LONI provides access to the Internet for the primary purpose of transmitting and sharing of information among governmental, research and educational organizations. Transmission of any material in violation of any federal or state laws or regulations is prohibited. Internet connections shall not be used to access other machines without the permission of the owner. The Subscriber agrees to observe the acceptable use policy of any other network the Subscriber accesses through LONI. LONI subscribers are expected to be responsible in their use of the network and avoid actions that cause interference to the network or cause interference with the work of others on the network.

9.1.5 Internet Server Policies

College web accounts (accounts hosted under the www.bpcc.edu domain) will adhere to the following policies:

9.1.5.1 *Accounts are created on College servers for the publishing of information related to departments, colleges, and organizations. No personal accounts will be allowed on these servers despite the connection between the organization and the staff. If a personal account is discovered, the site will be removed without warning to the publisher. Personal accounts are hosted free of charge on http://alpha.bpcc.edu and the Computer Services may be contacted for support in regards to personal accounts.* ***All accounts are subject to review for appropriateness to the mission of the College, the accuracy and legality of the published data, and consistency with College, Board, and state policies.***

9.1.5.2 *Each site will have a dedicated BPCC faculty / staff member as a contact for information regarding the site. Those members may solicit external help in the creation of their web site as long as they inform the webmaster who is performing changes to the site.*

9.1.5.3 *Accounts are created on the College server for organizational information publishing only. Any activity other than publishing must be approved by the webmaster. These activities include server-side script execution, server-side processing, and any other activity that relies on processing from the web server(s). Note that email links are appropriate as they are not processed on the web servers.*

Activities for Required Approval include, but are not limited to:

1. *CGI processing*
2. *Database Processing*
3. *Active Server Pages*
4. *Java Applications*
5. *Non-Email Forms Processing*
6. *Front Page component/element usage*

The webmaster reserves the right to remove any material found to be using unapproved elements. Access to the *server will be removed if such elements are found to exist. For any questions, please contact the webmaster.*

9.1.5.4 Account Disk Quotas will begin at 5MB per account. Requests for quota increases must be submitted for approval in writing to the Computer Services. These requests should justify the need for quota increase. All accounts over quota will be informed of their quota status and requested to remedy the situation in an allocated time period. If the situation is not remedied in the allocated period, access to the site will be removed.

Amended March 11, 1999

9.1.6 Second Tier Internet Servers

The Computer Services at BPCC is providing each college with a dedicated web server to facilitate independent site functionality that exceeds the provisions of the College web server (www.bpcc.edu).

The web server resides in G-161 and will have global access in front of the firewall. The server is remotely administrated and no physical access to the server is allowed without permission and supervision of the College webmaster or Computer Services.

The servers are provided with the understanding that the following below policies are met. Failure to adhere to the below policies will cause removal of permissions to the server by the Computer Services.

9.1.6.1 Access: *Second Tier Servers are designed to be remotely administrated by a dedicated Senior Systems Analyst. Physical access by unauthorized Computer Services personnel is a violation of current Bossier Parish Community College audit policies. Complete site functionality is available through remote access by the Senior Systems Analyst.*

9.1.6.2 Archiving / Restoration: *The Computer Services will maintain archiving of the server. Requests for restorations will need to be made to the Senior Systems Analyst. It is in the best interest of each party to maintain local archives in case of restorations.*

9.1.6.3 ODBC: *Each server is allowed one DSN for an ODBC connection. The source file should be placed in its permanent directory before requesting DSN mapping.*

9.1.6.4 Processing: *Each server provides the temporary owner full processing capabilities. The College webmaster reserves the right to remove any processing application from the server.*

9.1.6.5 Administrators: *Each temporary owner is provided with Administrator access to the server. The Administrator can freely create directories, control content, and develop the site in a manner in accordance with College policies.*

9.1.6.6 Additional Users: *Requests for additional users of the server should be made to the Senior Systems Analyst. User accounts will be created and documented.*

9.1.6.7 Disk Quota: *The provided server disk quota is currently 100MB. Requests for increasing the quota should be submitted to the Senior Systems Analyst for approval. A justification must accompany the request.*

9.6.8 College Presence: *Temporary owners of the web server must maintain required information on the College web server in tandem. These servers are provided for extended site functionality only. Personal accounts are not allowed.*

Naming Convention: The following domain names are available:

www.business.bpcc.edu

All servers and temporary owners must comply with guidelines stipulated by the Bossier Parish Community College Electronic Data Systems Policies and Standards. These policies are subject to amendments.

Amended March 16, 1999

9.2 **Telephone Service**

Bossier Parish Community College provides its own telephone service via an on campus switch and voice network

9.2.1 **General Guidelines**

Use of the College telephone network is provided to the College community subject to all applicable College, state, and federal usage guidelines. Violation of these guidelines may result in loss of usage privileges and/or disciplinary action.

Phones purchases, including the cost of network supplies, are the responsibility of the budget unit requesting phone sets or associated wiring.

All purchases of digital sets must be approved in advance though the Computer Services.

Repair and/or installation are the responsibility of the Computer Services. Requests for telephone associated maintenance should be directed to the Computer Services.

All repairs or maintenance of telephones or the telephone network is the sole responsibility of the Computer Services

9.2.2 **Usage Policies**

- Access to the campus telephone system is provided to College employees for business use only.

- Students may use non-office phones for personal use provided access to these phones is granted by permission from, or by contract with, the College.

9.2.3 **LINC Access**

- LINC access is to be used by authorized College personnel and is to be used for business only.

- Each month charges for LINC calls are presented by phone number to the individual or unit responsible for the phone from which the LINC calls were made. The party responsible for the phone will sign the *LINC Detail Report* verifying that the calls made from the phone were College business related. The individual to whom the LINC access is assigned is responsible for all calls made from the number.

- Failure to return the signed *LINC Detail Report* by the deadline will result in termination of LINC access until which time the signed report is returned to the Computer Services

- A budget unit should request in writing from the Computer Services LINC access, or termination of such access, for unit personnel

9.2.4 **Cell Phone Usage**

All employees must sign a Cell Phone Authorization Form upon receiving a cell phone agreeing to be taxed and agreeing to use the text messaging feature for business purposes only. Any employee who has a cell phone but is not being taxed must sign a monthly statement attesting to the fact that the employee only used the cell phone for business purposes only and that is the reason for excluding the employee from taxes.

9.3 **Computer User Accounts**

To use the BPCC computer resources, a user must first be assigned a computer account. Students, both undergraduate and graduate, are eligible for an account if they are enrolled at BPCC. All Bossier Parish Community College employees are eligible for computer accounts.

If a computer account has been assigned to a student and the student withdraws from the College, that account is no longer valid and will be terminated. Student accounts will be disabled between semesters. Once a student pays fees for the semester or session account access will be restored for that semester or session. If a student does not reenroll and pay fees for a successive semester the account will be terminated.

Computer accounts for academic and staff personnel will be terminated when the employee no longer has an active assignment within the College community.

Administrative, faculty, and staff user accounts are governed by the department/unit that the employee is assigned to. When the person's association with the department ends, that account will no longer be valid and will be terminated. Accounts for personnel on leave will be disabled for the duration of the leave period. Transferring from one department to another will not result in termination but rather a commensurate change in governance of the account. Department Heads are responsible for notifying the Personnel office <u>and</u> the Computer Services when an employee terminates employment, takes leave, or moves to another job assignment out side the department/unit.

9.4 **Acquiring a User Account**

To be eligible for a user account, the requester must meet one of the following qualifications:

Be enrolled in courses as a student at BPCC and have completed the fee payment process

Be employed as a faculty member at BPCC.

Be employed as a staff member at BPCC

Be employed as an administrator at BPCC

Any exception to the above will require the written permission of the College Chancellor.

To establish a user account:

Complete and submit to the Computer Services a *Request for User Account* form.

The system administrator or designee will verify that the requester is eligible for an account.

The System Administrator or designee will open the account and place an associated password and user name on the *Request for User Account* form

A copy of the *Request for User Account* form, containing the new account information, is released to the requester upon proof of identification and receipt of the requester's signature.

9.5 **User Name Scheme**

The following naming scheme will be followed in the assignment of computer usernames:

Faculty/Staff/Administrative – *First Initial* followed by *last name* will be used when possible. If already in use, *first and 2nd Initial* followed by last *name* will be used.

Example: JOHN W. SMITH

1ST – JSmith

2ND - JWSMITH

Each username will be placed in the appropriate group at time of creation. The group structure shown below will be followed:

101 – SISUSERS

100 – STAFF

101 – FACULTY

300 – STUDENTS

200 – ADMINISTRATORS

800 – TEST ACCOUNTS

3375 – GUEST ACCOUNTS

9.5.1 **Password Assignments**

A password will be assigned with every username. This password must be changed the first time a user logs on. If any user loses or forgets their password, he/she must request a password change from Director of Computer Services

9.6 **User Policy Summary**

Users of College information resources must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the privacy of other computer users. This policy is applicable to all College students, faculty, and staff and to any others granted use of Bossier Parish Community College resources. This policy refers to all College information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the College. This includes word processing equipment, personal computers, workstations, mainframes, minicomputers, and associated peripherals and software, regardless of whether used for administration, research, teaching, or other purposes.

9.7 **Locally Defined and External Conditions of Use**

Individual units within the College may define "conditions of use" for information resources under their control. These statements must be consistent with College EDP policy but may provide additional detail, guidelines and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. The individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

9.8 **User Responsibilities**

Access to the information resource infrastructure both within and beyond the College campus, sharing of information, and security of the intellectual products of the community, all require that each and every user accept responsibility to protect the rights of the community.

9.8.1 **User Accountability**

All users are solely accountable for all usage/activity associated with their respective account. This includes any electronic mail, data transfer, Internet sites accessed and personal web pages. The Computer Services reserves the right to access the information and/or content related to any user account with justifiable cause. Only the Computer Services Director can authorize this access.

9.9 **Governing Policies**

Note: *Any user of College information resources who is found to have purposely or recklessly violated any of the following policies will be subject to disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action.*

9.9.1 **Copyrights and Licenses**

Copying: All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any College facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

Number of Simultaneous Users: The number and distribution of software copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

Copyrights: In addition to software, all other copyrighted information (text, images, icons, programs etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media.

9.9.2 **Integrity of Information Resources**

Modification or Removal of Equipment: Technology users, including faculty, students, and staff, may not, in anyway, modify or remove computer or network equipment, software, or peripherals that are owned by the College/State without proper authorizations. Absolutely no modification may be made to any computer, or peripheral, or network device without the permission of the Computer Services and College Property Control unit.

Encroachment on Access and Use: Computer users must not encroach on others' appropriate access to, or use of, College computer or network devices. This includes but is not limited to: the sending of chain-letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a College computer or network, and damaging or vandalizing College property.

Unauthorized or Destructive Programs: Computer users must not intentionally develop or use programs which disrupt network or computer use, or which access private or restricted portions of a system and/or damage the software or hardware components of a system. Computer users must use great care to ensure that they do not use programs or utilities which interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than those permitted in the network guidelines.

Academic Pursuits: The College recognizes the value of research on game development, computer security, and the investigation of self-replicating code. The College may restrict such activities in order to protect College and individual computing environments, but in doing so will take account of legitimate academic pursuits.

9.9.3 **Unauthorized Access**

Abuse of Computing Privileges: Users of College information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the College. For example, abuse of the networks to which the College belongs or the computers at other sites connected to those networks will be treated as an abuse of Bossier Parish Community College computing privileges.

Reporting Problems: Any defects or abuse discovered in system accounting or system security must be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

Password Protection: A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system owner.

9.9.4 **Privacy**

Computer users must respect the privacy of other computer users. The College system provides mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to private information are violations of College policy and may violate applicable law. System administrators, will authorization from the Director of the Computer Services, may access computer users' files for critical maintenance purposes or in response to suspected policy violations. System administrators will report suspected unlawful or improper activities to the Director of the Computer Services.

Unlawful Messages: Use of electronic communication facilities (such as mail or chat, or systems with similar functions) to send fraudulent, harassing, obscene, threatening, or other messages that are a violation of applicable federal, state, or other law or College policy is prohibited.

Mailing Lists: Users must respect the purpose and charters of computer mailing lists (including local or network newsgroups and bulletin boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the list's purpose. Persons sending to mailing list any materials that are not consistent with the list's purpose will be viewed as having sent unsolicited material.

Advertisements/solicitations: In general, the College's electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations, or promotions (See Commercial Use, below)

Information Belonging to Others: Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of the other user and, where applicable, the permission of the system administrator and Director of the Computer Services.

Confidentiality: The College does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, individual users or the College may be required by law to provide electronic or other records or information related to those records or relating to use of information resources.

9.9.5 **Political, Personal, and Commercial Use**

The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, use of real estate and similar matters. It is also a contractor with government and other entities and thus must assure proper use of property under its control and allocations of overhead and associated costs. Use of the College information resources, including the use of the College computer network capabilities, are, therefore, subject to the following conditions:

Political Use: College information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal state and other laws and in compliance with applicable College policies.

Personal Use: College information resources may not be used for personal activities not related to College functions.

Commercial use: College information resources should not be used for commercial purposes except in a purely incidental manner or as permitted under other written policies of the College or with the written approval of a College officer having the authority to give such approval. Any such commercial use should be properly related to College activities, take into account proper cost allocations for government and other overhead determinations and provide for appropriate reimbursement to the College for taxes and other costs the College may incur by reason of the commercial use. Users also are reminded that the "EDU" domain on the Internet has rules restricting or prohibiting commercial use.

9.9.6 **Personally Identifiable Information**

Personally Identifiable Information (PII) –is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered PII is available in public sources such as telephone books, public websites, College listings, etc. This type of information is considered to be Public PII and includes:

1. First and Last name

2. Address

3. Work telephone number

4. Work e-mail address

5. Home telephone number

6. General educational credentials

7. Photos and video

In contrast, Protected PII is defined as any one or more of types of information including, but not limited to:

1. Social security number

2. Username and password

3. Passport number

4. Credit card number

5. Clearances

6. Banking information

7. Biometrics

8. Data and place of birth

9. Mothers maiden name

10. Criminal, medical and financial records

11. Educational transcripts

12. Photos and video including any of the above

(If a question arises about what is or isn't PII please contact the Computer Services Department at compservices@bpcc.edu)

B. BPCC Information System–a collection of computing resources that are accessible through privileged access such as a login or key. Usually a software package designed to store student and employee data. E.g. Banner, Canvas, Document Imaging, and databases.

C. Secure Deletion – Secure deletion of an electronic file is accomplished by overwriting the full file contents with random data multiple times.

X. Procedures

A. General

This section provides guidelines on how to maintain and discard PII. If current procedures fall outside this policy or questions arise please contact the Computer Services Department to suggest more efficient procedures for protecting PII.

All electronic files that contain Protected PII will reside within a protected BPCC information system location. All physical files that contain Protected PII will reside within a locked file cabinet or room when not being actively viewed or modified. Protected PII is not to be downloaded to personally owned, employee or contractor workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the college. PII will also not be sent through any form of insecure electronic communication E.g. E-mail or instant messaging systems. Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted. For help with secure deletion please contact the Computer Services Department at compservices@bpcc.edu.

B. Exceptions

If there is an operational or business need to store protected PII outside a BPCC controlled information system please contact the Computer Services Department at compservices@bpcc.edu for assistance in securing the information.

C. Incident Reporting

The Computer Services Department must be informed of a real or suspected disclosure of Protected PII data within 12 hours after discovery. E.g. Misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII.

D. Audits

Periodic audits of BPCC owned equipment and physical locations may be performed by the Chief Information Officer or delegates to ensure that protected PII is stored in approved information systems or locations. The purpose of the audit is to ensure compliance with this policy and to provide information necessary to continuously improve business practices.

XI. Enforcement

An employee found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation.

9.10 **System Administrator Responsibilities**

While the College of Louisiana System is the legal "owner" or "operator" of all computers and networks purchased or leased with College funds, oversight of any particular system is designated to the head of a specific subdivision of the College governance structure, such as a Dean, Department Chair, Administrative Department Head, Principal Investigator, etc. For College-owned or leased equipment, that person is the responsible administrator of the policies in this document.

The responsible administrator may designate another person to manage the system. This designee, is the "system administrator". The system administrator has additional responsibilities to the College as a whole for the system(s) under his/her oversight, regardless of the policies of his/her department or group, and the responsible administrator has the ultimate responsibility to see that these responsibilities are carried out by the designated system administrator.

The system administrator should use reasonable efforts:

To take precautions against theft of, or damage to the system components.

To execute all applicable hardware and software licensing agreements.

To treat information about, and information stored by, the system's users in an appropriate manner, and to take precautions to protect the security of a system or network and the information contained therein.

To promulgate information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.

To cooperate with the system administrators of other computer systems or networks, whether within or without the College, to find and correct problems caused on another system by the use of the system under his/her control.

To enforce applicable College EDP policy

9.10.1 **Policy Enforcement**

The system administrator is authorized to take reasonable action to implement and enforce the usage and service policies of the system and to provide for security of the system.

9.10.2 **Suspension of Privileges**

A system administrator may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of a computer system or network. The Computer Services has ultimate authority for policy enforcement over all systems owned by or associate with Bossier Parish Community College.

9.11 **Computer Services Director Responsibilities**

The College's Chief Information Officer (Director of the Computer Services) shall be the primary contact for the interpretation, enforcement and monitoring of this policy. Any legal issues shall be referred to the System Legal Office for advice.

9.11.1 **Policy Interpretation**

The Computer Services Director shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

9.11.2 **Policy Enforcement**

The Computer Services Director shall work with the appropriate administrative units to obtain compliance with this policy.

9.11.3 **Inspection and Monitoring**

Only the Computer Services Director or designee can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper use of computer or network resources.

9.12 **Consequences of Misuse of Computing Privileges**

9.12.1 **Cooperation Expected**

Users, when requested, are expected to cooperate with system administrators in any investigations of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.

9.12.2 **Corrective Action**

If system administrators have persuasive evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they should pursue one or more of the following steps, as appropriate, to protect other users, data files, and the computer network:

Provide notification of the investigation to the College's Computer Services Director, Vice President of Student Affairs (in the case of student use), the user's instructor, department or division chair, and/or supervisor.

Temporarily suspend or restrict the user's computing privileges during the investigation. A student may appeal such a suspension or restriction and petition for reinstatement of computing privileges through the Dean of Students. A staff member may appeal through applicable grievance procedures. Faculty members may appeal through the Dean of their college. Final decisions for reinstatement will be made by the Chancellor in consultation with the Director of the Computer Services.

With authorization from the College's Computer Security Officer or designate, inspect the user's files, diskettes, tapes, network use logs, and/or electronic account(s).

Refer the matter for possible disciplinary action to the appropriate College unit, i.e., the Vice President of Students for students, the appropriate supervisor for staff, and the Dean of the relevant College for faculty or other responsible teaching or research personnel.

9.13 **Student Access/Use Policies**

The use of College computer/network facilities, including the BPCC network for Internet access, for any reason other then for College related activities, is strictly forbidden. Violators may lose access to College facilities and/or the College network and be subject to state or federal civil or criminal penalties.

For policy violations involving a student, referring the case to the Computer Services and to the Vice President of Student Affairs Office is the recommended course of action. This ensures that similar offenses may be considered for similar disciplinary action, from semester to semester, year to year, and instructor to instructor. It also allows the detection of repeat offenders.

10.0 Electronic Course Development and Implementation Policies*

The electronic course development and implementation policies are designed to facilitate the most efficient use of current technologies in order to meet the academic and administrative needs of the College. Specifically, the policies are intended to eliminate needless duplication of technologies, minimize support costs, ensure hardware/software compatibility, ensure data security, and comply with standards set forth by all recognized external governing agencies.

A course may not be delivered electronically without prior approval from the Board of Regents. Approval from the Board will be solicited through Continuing Education each semester in accordance with the procedures set forth by Continuing Education.

While the use of the Internet to augment a course is encouraged, classes must meet face to face at the time specified and for the scheduled duration.

It is not the instructor's prerogative to turn a course that has not been approved for electronic delivery into an n electronic course.

All Internet/Web based courses must use the course management/gateway software package(s) approved by the College.

All Internet courses will be hosted on designated secure College servers, which are managed and supported by the Computer Services in accordance with approved electronic data processing policies and procedures.

All purchases of data processing technologies, including computer hardware, software, peripherals or networking devices must be approved in advance by the College Computer Services's technical support and review committee.

Electronic delivery of course material must comply with all applicable copyright laws.

All electronic courses must adhere to the standards set forth by the Southern Region Electronic Campus (SREC), Southern Association of Colleges and Schools (SACS), the Louisiana Board of Regents, the Board of Supervisors for the College of Louisiana System and Bossier Parish Community College.

*For the purpose of this document electronic course delivery includes the use of all forms of electronic technologies including the internet, computerized programs, CD-ROMS, video tapes, audio tapes, television, radio, satellite, audio-graphics, and compressed video.

11.0 **Acquisition of Computer Hardware, Software, and Services**

The Computer Services's Technical Support and Review Committee (TSRC) will review all proposed purchases of data processing, or other information technologies, including computer hardware, software, peripherals or networking devices in order to ensure: (a) that acquisitions will satisfy the need, (b) completeness of the request; (c) compatibility of hardware/software, and (d) supportability. It is not the purpose of the committee to thwart purchases/grants but rather to assure their technical quality and appropriateness.

The Technical Support and Review Committee is composed of the technical staff employed by the Computer Services and works in cooperation and consultation with the unit making the purchase request. The committee will meet every Tuesday and Thursday to review purchase requests and grant applications.

All purchase requisitions (PRs) and grant applications involving any information technologies must be approved through the Computer Service's Technical Support and Review Committee. Grant applications will be routed to the Technical Support and Review Committee through Grants and Contracts. **(Grant applicants are advised to discuss the technical aspects of a grant well in advance. The Technical Support and Review Committee will not be responsible for delays in grant process if adequate time is not provided for review and possible modification of the grant application.)** Upon approval by the committee, the PR/grant application will be forwarded to the appropriate agent for signature approval. Business Affairs will not accept any purchase requisition for information technology that has not been pre-approved by the Technical Support and Review Committee.

11.1 ***Expenditures Requiring Review***

The following technology commodities/services have been identified by expenditure object code as those requiring review and approval through the Technical Support and Review Committee (TSRC) prior to submittal to Business Affairs/Purchasing Section for processing:

3330 Maintenance of Data Processing Equipment: *Maintenance and minor repair of data processing equipment performed by an outside agent or agency, includes service contracts and repair on/for personal computer systems and Computer Services hardware, including peripherals and systems software.*

3430 Rentals - Data Processing Equipment: *Rentals and/or lease of data processing equipment for offices and Computer Services.*

3435 Computer Software: *Cost incurred in the acquisition of computer software, when purchased separately from computer hardware.*

35l3 License Fees: *Software license fee, taping license, broadcasting fee, etc. Telephone & Telegraph: All charges included in the Standard bill"for telephone services. This would include standard state services, local and LINC; business services, local and long distance; cellular services; and 800 services.*

3711 Telephone - Local Service: *Charges for local service.*

3712 Telephone - Long Distance Service: *Charges for long-distance service.*

3713 Telephone - Linc Charges: *Linc Service*

3714 Telephone - Service Contract: *Charges for service contract on maintenance of College telephone systems.*

3715 LA NET/LA Linc: *Charges for LA NET/LA Linc service.*

3716 Data Lines and Circuits: *Any charges for data lines, circuits, and Wide Area Networks.*

3719 Telephone - Other: *Other charges for maintaining the College's telephone systems, not otherwise specified.*

3720 Telephone Base Charge: *Base charge for telephone usage.*

3730 Telegraph: *Charges for telegraph, teletype, fax charges, etc.*

3740 Other Communication Services: *Charges for other services other than telephone, and data line or circuits which would include radio paging, OTM credit card, etc.*

3985 Transponder Time: *Charges for transponder time.*

4471 Computer Supplies (Technology): *Supplies used to upgrade and/or monitor a system's hardware or peripherals. For example: motherboards, processors, memory, power supply, Ethernet cards, sound cards, SCSI devices, CD-ROM, internal zip drives, internal modems, CD units hubs, keyboards, external zip drives, external modems, etc.*

5775 Computer Related Consulting: *Professional services contracts for networking services, including consulting.*

7260 Medical: *Equipment used in the treatment or diagnosis of sick or injured, including veterinary equipment, and veterinary & medical equipment with computer related operation. Cost would include purchase price, delivery charges, taxes, installation charges and other purchase-related costs.*

7275 Computers (Purchases over $250): *Computer hardware, including peripherals. Common items are: computers, scanners/all in one, printers, UPS, hubs/SCSI devices, routers, photographic/digital cameras, etc.*

7280 Educational, Recreational & Cultural: *Equipment used for educational, recreational or cultural enrichment. Common items are: overhead projectors, artifacts for museums, pool tables, weights, TVs, VCRs, musical instruments, video servers, smart boards; and any* *video/audio/classroom equipment that is connected to computers. Cost would include purchase price, delivery charges, taxes, installation charges and other purchase-related costs.*

7310 Communications: *Equipment used for communications such as radios, antennas, teletype machines, aircraft guidance systems, satellite equipment, telephone system add-ons, etc. Costs would include purchase price, delivery charges, taxes, installation, microphones, and other purchase-related costs.*

Approval Process for the Electronic Data Systems Policies and Standards:

Approval by Director of the Computer Services

Approval by College Chancellor

Distribution for the Electronic Data Systems Policies and Standards:

Notification of On-line Access

Budget Unit Heads

Regular Faculty

Adjunct Faculty

College Staff

Students

Grant Employees