Blue Mountain Community College
Administrative Procedure

Procedure Title: **Use of College Electronic Information Resources**
Procedure Number: 04-2004-0001
Board Policy Reference: IV.A.

Accountable Administrator: **Vice President for Information Technology**
Position responsible for updating: Vice President for Information Technology
Original Date: May 15, 1996
Date Approved by Cabinet: 3-20-07
Authorizing Signature: *signed original on file*
Dated: 04-13-04; 03-21-07
Date Posted on Web: 03-23-07
Revised: 02-19-07
Reviewed:

Purpose:

This statement establishes measures for the protection of, access to, and acceptable and responsible use of Blue Mountain Community College's electronic information resources (EIRs). EIR's include, but are not limited to: email, voice mail, fax, telephone, interactive television (ITV), copiers, printers, computers and associated storage devices.

Principles:

The electronic information resources at BMCC are to be used in a manner that supports the educational mission of the college. By mission and policy, BMCC encourages learning, research, creativity, teaching, and the free exchange of ideas in a climate of openness and sharing.

Electronic information technologies are an important set of tools in this effort. Users must show respect for college property, consideration of others, responsibility for actions, and authorized and efficient use of college resources. EIR's must be used in compliance with international, federal, state, and local laws and for college-related purposes and activities as defined by custom, contract, and board policy and procedure.

BMCC can not guarantee that messages or files are private or secure. All data and software housed on college EIRs becomes the property of BMCC within license and copyright restrictions and must comply with contract agreements between BMCC and its employee associations.

Users shall be responsible for messages that they transmit through the college's EIRs and shall obey the acceptable use policies of the Internet and any rules of discussion forums in which they participate. Fraudulent, harassing or obscene messages and/or materials as defined by contemporary court decisions are not to be sent or stored.

Definitions:

Electronic Information Resources (EIRs): All electronic hardware, software and associated data that support the following: administrative information systems, desktop computing, library automation; multi-media, data video and voice networks; electronic mail (e-mail), Internet access; modems; scanners; telephone systems; voice mail; and any other functionality purchased and/or contracted for by the college.

User: Any person authorized to use the college's electronic information resources.

Authorized Accounts: Username/password pairs or similar codes or code devices such as copy cards that allow a person access to an EIR.

Authorized Location: EIRs that have been approved for the storage and delivery of BMCC-related content.

Server: A server is a general-purpose computer system that is running one or more applications that allow remote access to data or remote control of the system. This includes, but not limited to computers running: PCAnywhere, Remote Desktop, VNC, or Timbuktu.

Acceptable Usage:

In order to make possible the widest use of these important technologies, a set of shared understandings and rules is necessary. In general, the same ethical conduct that applies to the use of all college facilities applies to the use of electronic media. Users must show respect for college property, consideration of others, responsibility for actions, and authorized and efficient use of college resources. In addition, users of EIRs must have a basic understanding of the role of the law regarding copyright and other legal issues.

1. College EIRs must always be used in compliance with all international, federal, state, and local laws.
2. EIRs are to be used through authorized accounts. Users must not share their authorized accounts with others in a manner that jeopardizes the security or integrity of the EIR. All violations of this policy will be treated as the sole responsibility of the owner of that account.
3. Users must respect the privacy of others by not inspecting, broadcasting, or modifying EIRs assigned to individuals without permission.
4. BMCC's EIRs must be used for college-related purposes and activities as defined by custom, contract and board policy, although occasional personal use is permitted.
5. The college cannot guarantee that messages or files are private or secure.
6. Network and system utilization activity may be monitored for purposes of maintaining system performance and security.
7. All data must be treated as confidential unless designated or authorized for public release. Data will generally be shared among those users whose work can be done more effectively by knowledge of such information unless prohibited. Access to data is not approval for its use outside an individual's official college responsibility.
8. No one shall deliberately attempt to degrade the performance of an EIR or block access to others.

9. No one shall knowingly introduce invasive computer software such as viruses on media that are brought into the college.
10. All data and software housed on college EIRs must comply with contract agreements between BMCC and its employee associations, and must comply with federal and international copyright law.
11. Users shall be responsible for messages that they transmit through the college's EIRs and shall obey the acceptable use policies of the Internet and any rules of discussion forums in which they participate. Fraudulent, harassing or obscene messages and /or materials as defined by contemporary court decisions are not to be sent or stored.
12. Information that is published electronically using World Wide Web, Kiosks, Bulletin Board Systems, or similar electronic applications for broad general consumption outside of the college shall be subject to the same standards as conventional publications with respect to the representation of the college.
13. All BMCC-related material shall be approved by the appropriate administrative office for content, format, and authorized location prior to publication.
14. Servers or workstations action as servers will only be used with the prior authorization of the Information Technology department.

Failure to abide by this procedure may result in temporary or permanent denial of access to BMCC's EIRs. Punitive or legal action may also be taken by the appropriate administrative or judicial body in accordance with college policies and bargained agreements.

Procedure:

Authorized BMCC employees will be granted access by the Human Resources Department (HR). HR will contact the HELP DESK and request an authorized account for each employee. A work order will be issued for the HELP DESK to set up the requested account for that employee.

BMCC constituents may utilize open computer laboratories and library public access EIRs in accordance with the principles and rules spelled out in this document.

Security of data and information stored on BMCC EIRs is essential. Authorized users are responsible for ensuring that unauthorized access and use is not allowed on EIRs under their responsibility.

Departmental servers may be authorized for use once a completed Departmental Server Authorization Form has been received and approved by the VP of Information Technology. Unauthorized servers will be removed from the network.

Special Forms: Departmental Server Authorization

Departmental Server Authorization Form

Blue Mountain Community College procedures require that all servers (see definition below) attached to the College network will be authorized by Information Technology before use.

Purposes:

The primary purposes of this process are to ensure:

- Security for the network, the servers, and other equipment attached to the network, and
- Safeguarding of the integrity, security, and confidentiality of BMCC data.

Definition of server:

A server is a general-purpose computer system that is running one or more applications that allow remote access to data or remote control of the system. This includes, but not limited to computers running: PCAnywhere, Remote Desktop, VNC or Timbuktu.

Send completed forms to: Robert Tally at rtally@bluecc.edu. Phone 278-5830 if you have any questions about completing the form.

The server administrator will be responsible for the following:

- Ensure that approved security measures remain in place;
- Keep the server and all of its software current with security patches;
- Maintain up-to-date antivirus software and definitions;
- Maintain operating systems at the level recommended by the vendor;
- Schedule and maintain backups for server configuration and contents to ensure timely recovery from a system failure;
- Develop a disaster recovery plan or contingency plan that includes steps that will be taken to ensure integrity of the data on the server and steps that will be taken to ensure continuing service in the timeframe required by the services provided on the server;
- Update server information annually;
- Notify Information Technology when the server is taken out of service.

By signing this form, the department head or unit supervisor...

- Agrees and ensures that Information Technology may conduct reasonable security testing of the server before it is made available externally and periodically thereafter;
- Agrees and ensures that, if a significant security weakness is identified, the server will be disconnected from the network until that weakness has been rectified;
- Assumes full responsibility for ensuring that the content of the server complies with all relevant local, state, and federal laws (including, but not limited to, those governing copyright, trademark protection, and software licensing);
- Apprises Information Technology of all changes in contact information for management and technical support for the server;
- Certifies that information about students, faculty, employees, and clients (past, present or prospective) does not reside on the server. Seek exemption from this requirement if there are compelling reasons for having such information on the server;
- Certifies the safeguarding of all backups and copies of BMCC data.

Department Information

Dept Name:	Date:
Dept Address:	Dept Phone:
Dept Email (if any)	
Department Head or Unit Supervisor:	
Title:	
Signature:	

Administrator Contact Information

The primary and backup administrator contact information is required. You may provide other technical support contacts. All administrators and other technical support contacts will be contacted if there is a problem detected with the server

Primary Server Administrator Name:	Phone:
Email:	Office (Building and Room):

Backup Server Administrator Name:	Phone:
Email:	Office (Building and Room):

Other Technical Contact Name:	Phone:
Email:	Office (Building and Room):

Other Technical Contact Name:	Phone:
Email:	Office (Building and Room):

Server Information

Please provide basic information about the server. Include a brief description of how the server will be used, and an outline of the contingency plan, the room number where it is located, the type of hardware (PC, Mac, Sparc, etc.), the operating system (including version). ***No SMTP relay to the approved BMCC email server will be authorized or used.***

Server Name:	Date Operational:	Date Retired:	□ New □ Update
Purpose:			
Contingency Plan: (Include information on how important the server is, how long it can be down, and the general plan for recovery when there is a hardware failure			

Server Location:	Hardware:	Operating System:

Network Information
Please provide the following for each network interface card in use on the server.

IP Address	MAC Address	DNS Name (if any)

* If the server connects to the network via a wireless access point, please list the MAC address of the wireless network interface card in the server, not the MAC address of the access point.

Services

For each service running on the computer, please provide the following information. The name of the application (including version number), what protocols (TCP, UDP, etc.) and ports it is running on, any special DNS name associated with the service, and indicate whether this service should be accessible from the Internet.

Application	Protocol	Ports	DNS Name	Internet Accessible

Information Resources Use

Received:	Approved:	Firewall Changed: