Blue Mountain Community College

Administrative Procedure

Procedure Title: **BMCC Acceptable Use**
Procedure Number: **04-2019-0002**
Board Policy Reference: **IV.A.**

Accountable Administrator: **VP Administrative Services**
Position responsible for updating: **AVP Information Technology**
Original Date: 01-22-2020
Date Approved by College Planning Council: 01-22-2020
Authorizing Signature: *signed original on file*
Dated: 01-22-2020
Date Posted on Web: 01-23-2020
Reviewed:

Overview

The Acceptable Use Administrative Procedure is not to impose restrictions that are contrary to Blue Mountain Community College's (BMCC) established culture of openness, trust and integrity. This Procedure is committed to protecting BMCC's staff, faculty and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing file sharing, shared drives, electronic mail, web searches, file uploads and downloads, are the property of BMCC. These systems are to be used for business purposes in serving the interests of the college, and of our students and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every BMCC employee, faculty member, and partner who deals with information and/or information systems. It is the responsibility of every computer and information user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this Procedure is to outline the acceptable use of technology equipment and information assets. These rules are in place to protect the staff, faculty and the college. Inappropriate use exposes the college to risks including virus attacks, compromise of network systems and services, significant financial penalties and legal issues.

The college is responsible for compliance with a number of laws, regulation, and orders which affect the way we must handle information. The college will comply with these external mandates and will execute the actions and maintain the necessary policies and organizational structure required to do so.

External mandates include, but are not limited to Federal laws:

- HIPAA (Health Insurance Portability and Accountability Act)
- FERPA(Family Educational Rights and Privacy Act),

- GLBA (Gramm-Leach-Bliley Act)
- PCI/DSS (Payment Card Industry Data Security Standard)
- HITECH (Health Information Technology for Economic and Clinical Health) Acts

State of Oregon privacy laws and practices

Scope
This Procedure applies to the use of all information assets, electronic and computing devices, and network resources to conduct the college business or interact with internal/external networks and business systems, whether owned or leased by BMCC, the staff, the faculty, student/temporary staff and faculty or a third party. All staff, faculty members, contractors, consultants, temporary, and other workers at BMCC are responsible for exercising good judgment regarding appropriate use of information assets, electronic devices, and network resources in accordance with BMCC policies and standards, and local laws and regulation. Exceptions to this Procedure are documented under the section titled "Administrative Procedure Compliance"

Program

Information Access Control

Need to Know
Access to information in the possession of, or under the control of BMCC must be provided based on the need to know. Information must only be accessed or disclosed to people who have a regular job function with a business need for the information.

Access Approval
To implement the need-to-know concept, BMCC has adopted an access request and approval process. Users must not attempt to access sensitive information unless the relevant custodian has granted them access rights. When a user changes job duties, including termination, transfer, promotion and leave of absence, his or her supervisor must immediately notify the Human Resources Specialist. The privileges granted to all users will be annually reviewed by information custodians to ensure that only those with a current need to know presently have access.

User IDs and Passwords
All user access is logged and monitored. Each user is personally responsible for the usage and protection of his or her user ID and password, and users must not share credentials. A user must change their password immediately if they suspect that it has been discovered or used by another person. Users must notify Information Technology if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

Information Security

Protecting Information
Information security is an institutional priority and a shared responsibility among all academic departments, administrative offices and third party service providers. Each administrative office and academic department is responsible for the stewardship of confidential, sensitive and/or personally identifiable information (PII) used within the context of college operations and academic programs, and must limit physical and electronic access privileges to authorized personnel based on a regular job function with a business need for the information to individuals whose active employment status and/or affiliation with the college can be verified. Each user has an obligation to protect personally identifiable information (PII) from unauthorized viewing or dissemination. No user should independently decide to

share sensitive information with another user. Examples of potentially sensitive information, not limited to, but include the following:
Names
Addresses
Social Security numbers
Credit card information
Date of Birth
Driver's license number
Grades
Financial aid
Health records
Counseling records
Network logins
Student information
Employee information
Applicant information
Communications (who sends to who)
E-mail content
Research
Donor information

Handling Of Sensitive Personally Identifiable Information
Sensitive or confidential information, in any form or media, must not leave BMCC offices without prior approval from the Vice President of Administrative Services. If it is necessary to remove computer-readable sensitive information from BMCC offices, this information must be protected with encryption facilities approved by Information Technology. If sensitive information is transmitted over public computer networks such as the Internet or email, this transmission must take place with encryption facilities approved by Information Technology. All portable and remote systems storing sensitive BMCC information must also employ hard disk encryption systems.

Harassment
BMCC's harassment policy, on-line and as printed in the catalog and schedule, extends to the networked world. For example, sending unsolicited or repeated electronic messages that unreasonably interfere with anyone's education or work at BMCC may constitute harassment.

BMCC's policy and state and federal statutes prohibit unwanted sexual behavior, lewd or indecent conduct, and behavior defined as "stalking." Electronic versions of these behaviors are also prohibited.

Intentional transmission or display of unwanted messages, information, or graphic images, which create a hostile academic or work environment are inappropriate uses of College electronic resources and violate BMCC's policy on harassment, as well as federal and state laws.

Privacy Disclaimer
Employees should adhere to any applicable federal and state laws concerning storage, retention, and destruction of data. Institutional data shall be used only for legitimate business of BMCC.

Individual, student educational records are protected by the Family Educational Rights and Privacy Act (FERPA). Disclosure of student records information to any person or agency outside of BMCC shall be approved by the Director, Enrollment Services/Registrar, the records custodian.

All users will respect the privacy of others by refraining from inspecting, broadcasting, or modifying

personal data files without the prior consent of the individuals involved.
Computer activity, including Internet usage, is monitored by authorized individuals for purposes of maintaining system performance and security. In instances when individuals are suspected of abuse of computer usage, the contents of user files may also be inspected.

E-mail messages are not necessarily protected from disclosure. It is possible for messages protected by a password or which have been deleted to be accessed by others.

All e-mail messages are ultimately considered college property. There shall be no expectation of privacy or confidentiality in electronic communications.

BMCC will make every effort to ensure the integrity of its various systems. Safeguards are maintained; however, no system can ensure absolute system security. Thus, users should not rely on system safeguards to ensure privacy or integrity of information stored or transmitted.

Physical Security

Positioning Display Screens
The display screens for all personal computers used to handle sensitive or confidential data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see workers enter passwords, encryption keys, and other security-related parameters.

Locking Sensitive Information
When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

Procedure

General Use and Ownership
BMCC information stored on electronic and computing devices whether owned or leased by BMCC, the staff and faculty or a third party, remains the sole property of BMCC.

Users must ensure, through legal or technical means, that information is protected in accordance with all relevant Administrative Procedures.

Users have a responsibility to promptly report the theft, suspected theft, loss, suspected loss or potential and known unauthorized access or disclosure of BMCC sensitive information.

User are responsible for exercising good judgment regarding the reasonableness of personal use of BMCC equipment. If there is any uncertainty, staff and should consult their supervisor or manager.
For security and network maintenance purposes, authorized individuals within BMCC may monitor equipment, systems and network traffic at any time.

Loopholes in security systems or knowledge of a special password are not to be used to alter information systems, obtain extra resources, take resources from another user, gain access to systems, or use systems for which proper authorization has not been given.

Users without proper authorization should never access or attempt to access any computer/network equipment, data, or software. **Access** includes, but is not limited to reading, writing, creating, deleting, modifying or copying of data, or moving, connecting, or disconnecting cables, devices or Wi-Fi, changing equipment settings, or wiretapping. **Data** includes, but is not limited to printouts, contents of electronic or removable media, or and other physical computer media, data communications, or data repositories.

System management techniques should be used by all levels of college staff to ensure that
(a) the integrity of information is preserved through access controls and data custodianship assignments;
(b) system capabilities can be reestablished within an appropriate time frame upon loss or damage by accident, malfunction, breach of security, or natural disaster; and
(c) actual or attempted breaches of security can be detected promptly.

BMCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this Procedure.

Fulfillment of public information requests should follow the Access to Public Records Administrative Procedure.

Security and Sensitive Information
All personal mobile, computing and storage devices that connect to the internal network must comply with the Acceptable Use Procedure.

System level and user level passwords must comply with the Password Procedure. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices accessed by staff, faculty and student/temporary employee must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.

Postings by staff and faculty from a BMCC email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of BMCC, unless posting is in the course of business duties.

Staff and faculty must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use
The following activities in general are prohibited. Staff and faculty may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a staff or faculty member of BMCC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing BMCC-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by BMCC.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which BMCC or the end user does not have an active license is strictly prohibited.

Accessing data, a server or an account for any purpose other than conducting BMCC business, even if users have authorized access, is prohibited.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your credentials/account by others. This includes family and other household members when work performing work.

Using a BMCC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

Making fraudulent offers of products, items, or services originating from any BMCC account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

Port scanning or security scanning is expressly prohibited unless prior notification to BMCC is made.

Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

Circumventing user authentication or security of any host, network or account.
Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Providing information about, or lists of, BMCC staff and faculty to parties outside BMCC.

Email and Communication Activities
When using college resources to access and use the Internet, users must realize they represent the college. Whenever staff and faculty state an affiliation to the college, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the college". Questions may be addressed to the Public Relations Office.

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone, texting or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of email header information.

Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited email originating from within BMCC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by BMCC or connected via BMCC's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media
Blogging by staff and faculty, whether using BMCC's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Procedure.

Limited and occasional use of BMCC's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate BMCC's policy, is not detrimental to BMCC's best interests, and does not interfere with an employee's regular work duties. Blogging from BMCC's systems is also subject to monitoring.

BMCC's Dissemination of College Information and Press Releases Administrative Procedures also applies to blogging. As such, staff and faculty are prohibited from revealing any BMCC confidential or sensitive information, trade secrets or any other material covered by BMCC's Marketing policies when engaged in blogging.

Staff and faculty shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of BMCC and/or any of its staff, faculty or students. Staff and faculty are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by BMCC's Non-Discrimination Statement and Anti-Harassment Policy.

Staff and faculty may also not attribute personal statements, opinions or beliefs to BMCC when engaged in blogging. If a user is expressing his or her beliefs and/or opinions in blogs, the user may not, expressly or implicitly, represent themselves as an employee or representative of BMCC. Staff and faculty assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, BMCC's trademarks, logos and any other BMCC intellectual property may also not be used in connection with any blogging activity.

Copyright - License
Copyrighted software is not to be copied from, into, or out of by using BMCC information systems, except as permitted by law and by the contract or license agreement with the owner of the copyright. The use of software on a local or a wide-area network or on multiple computers shall be in accordance with the license agreement.

All data and software used on BMCC information systems must comply with federal and international copyright law.

Liability Disclaimer for Lost Data
BMCC will attempt to plan for and advise users of scheduled down time; however, information resources can and will go down at unplanned times, and BMCC can assume no liability for any data lost or unavailability of data.

BMCC assumes no liability for lost revenue, lost data, lost output, time delay, system performance, software performance, incorrect advice from a consultant or other damages arising from the use of BMCC information resources, either on-site or remotely. Signing this agreement releases BMCC from any claim.

Administrative Procedure Compliance

Compliance Measurement
The Information Technology team will verify compliance to this Procedure through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the Vice President of Administrative Services.

All users must take all mandatory security and compliance training as directed by the college, and within the prescribed frequency.

Exceptions
Any exception to the Procedure must be approved by the Vice President of Administrative Services in advance.

Non-Compliance
An employee found to have violated this Procedure may be subject to disciplinary action, up to and including termination of employment. BMCC reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. To the extent permitted by law, BMCC reserves the right not to defend or pay any damages awarded against employees, faculty members or partners that result from violation of this Procedure.

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.

Information Asset: Any BMCC data in any form, and the equipment used to manage, process, or store BMCC data, that is used in the course of executing business, regardless if the data is stored on-campus or in an off-site or cloud environment.

Partner: Any non-employee or contractor of BMCC who is contractually bound to provide some form of service to BMCC.

Password: An arbitrary string of characters that is used to authenticate the user when he/she attempts to log on, in order to prevent unauthorized access to his/her account.

Sensitive Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[1]

System Administrator: An employee or partner who is responsible for managing a BMCC multi-user computing environment. The responsibilities of the system administrator typically include installing and configuring system hardware and software, establishing and managing user accounts, upgrading software and backup and recovery tasks, as appropriate.

User: Any BMCC staff, faculty member, student/temporary employee or partner who has been authorized to access any BMCC electronic information resource.

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 and information. 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 account information with others in a manner that jeopardizes the security or integrity of the EIR. Any violation of this Procedure 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. 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 approved for 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.

[1] National Institute of Standards and Technology Special Publication 800-122

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 they transmit through College 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 the internet, portals, 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. BMCC does not exercise control of material available on the Internet, some of which may be offensive to network users.
14. All BMCC-related material shall be approved by the appropriate administrative office for content, format, and authorized location prior to publication.
15. BMCC constituents may utilize open computer laboratories and library public access EIRs in accordance with the principles and rules spelled out in this Procedure.
16. 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.

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 bargaining agreements.

If you are not sure whether an activity or action you are planning would violate this Acceptable Use Administrative Procedure, you may contact the Associate Vice President of Information Technology at (541) 278-5783. Users who need help understanding this Procedure or who discover a violation of it should notify the Director of Human Resources at (541) 278-5947, or the Vice President of Administrative Services at (541) 278-5850.

Process:

Authorized BMCC staff and faculty will be granted access by the Human Resources Department (HR). HR will contact the IT Help Desk and request an authorized account for each user. A work order will be issued for the Help Desk to set up the requested account for that user, assuring that any required authorizations are secured.

By signing below, I (Print Name) _____ acknowledge that I have read and understand BMCC's Acceptable Use Administrative Procedure and agree to abide by this Procedure; and understand that violations of this Procedure may result in disciplinary action, up to and including termination.

_____ _____

Signature Date

Appendix A

External Mandates

Federal Family Educational Rights and Privacy Act (FERPA)

The federal Family Educational Rights and Privacy Act of 1974 (FERPA) provides a post secondary student the right to inspect his or her educational records and establishes the conditions concerning the disclosure of those records to third parties. Although the act does not specifically require that information security be implemented, the protection of electronic student records will require information security covering the student records subject to this federal law.[2]

Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act; GLB Act; GLB) Safeguards Rules

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLB Act), includes privacy provisions to protect consumer information held by financial institutions. In 2003, the Federal Trade Commission (FTC) confirmed that higher education institutions are considered financial institutions under this federal law. As of May 23, 2003, colleges and universities must be in compliance with provisions of the GLB Act that relate to the Safeguards Rule. Colleges and universities that already comply with the Family Educational Rights and Privacy Act (FERPA) will be deemed to be in compliance with FTC privacy rules under the GLB Act. (http://www.educause.edu/Resources/Browse/GLBAct/33353)

Health Insurance Portability and Accountability Act (HIPAA) Security Rules

The Health Information Technology for Economic and Clinical Health Act (HITECH), passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA), expands the application of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPPA) security rules to include "business associates" as well as "covered entities". As a result of the HITECH act, both need to implement written, comprehensive information security programs that address each aspect of the HIPAA security rule. In the higher education arena, HIPAA often applies to human resource offices and health services clinics used by both students and staff and to academic medical centers.

Payment Card Industry Data Security Standard (PCI/DSS)

In addition to the forgoing laws and regulations, the payment card industry created a private contractual compliance requirement: the Payment Card Industry Data Security Standard (PCI/DSS). The PCI/DSS requires that all merchants, including colleges and universities, that use credit cards comply with a number of administrative, technical and physical requirements. Failure to comply with the PCI/DSS could result in large penalties and suspension of the right to use credit cards for payment purposes.[3]

Oregon State Privacy Laws and Practices

https://www.ode.state.or.us/wma/alder/datagovernance_stateprivacylawsandpractices.pdf

[2] M. Peter Adler, "A Unified Approach to Information Security Compliance," EDUCAUSEreview September/October 2006

[3] M. Peter Adler, "A Unified Approach to Information Security Compliance," EDUCAUSEreview September/October 2006