BERKSHIRE COMMUNITY COLLEGE

Version: 1.1.4
Issued: 1/14/20

Acceptable Use Policy – BCC03

PURPOSE

The purpose of this policy is to define the acceptable use of Berkshire Community College's (BCC) Information Technology Resources (ITRs) including computer applications, hardware, email, telephony, and other systems by BCC employees, students, contractors, and third parties.

SCOPE

This policy applies to all BCC employees, students, contractors, and third parties who have been granted permission to access BCC systems. This policy applies to the entire College Network and all related equipment and is intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to these services.

POLICY

General Use

Access to ITRs is a key element in facilitating the productivity and creativity of users. As such, users are encouraged to use BCC information technology to the fullest extent in pursuit of the organization's goals and objectives. Access to College owned or operated ITRs imposes certain responsibilities on users and is granted subject to College policies and Commonwealth and federal laws. Appropriate use should always be legal, ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared resources. Use of these services should demonstrate respect for intellectual property, data ownership, system security, and individuals' rights to privacy and to be free from intimidation, harassment, and unwarranted annoyance.

BCC electronic communications systems, including intranet, Internet, telephony, email, and messaging services, are to be used for instructional and work-related purposes.

Access

Users of BCC information systems are authorized to access only those systems, including hardware and software, where their access has been previously approved.

Remote Access and Mobile Devices

As BCC continues to expand its information technology capabilities users with a College-related need may have the opportunity, with authorization from their managers and the CISO, for remote access to email and other applications through BCC provided or their own, personal devices. Access is authorized for the same purposes as all other BCC resources, i.e. College business and instructional use. Managers will approve remote access only for those users with a job-related need to access BCC resources remotely. Users who have been approved for remote access or mobile device privileges are responsible for adhering to the requirements defined in the BCC Mobile Device and Remote Access Policies.

Encryption

Occasionally users may have a business need to transfer or store, in a secure manner, information classified as confidential or restricted. In these instances, that information must be protected using encryption methods that have been approved and are identified in BCC's encryption standards. Users who may be unfamiliar with using encryption technologies should seek guidance from IT personnel.

Computer Virus and Malware Protection
It is important that users take particular care to avoid compromising the security of the network. Users will exercise reasonable precautions in order to prevent the introduction of a computer virus or other malware into the BCC network. Virus scanning software is installed on all BCC systems and is used to check any software downloaded from the Internet or obtained from any questionable source. Users are prohibited from disabling, or attempting to disable, virus scanning software. Additionally, executable files (program files that end in ".exe") will not be stored on, or run from, network drives or computers connected to the BCC network. Users must scan portable media devices for viruses and malware before using them to see if they have been infected. If staff members are unsure of how to utilize virus and malware scanning tools it is recommended that they contact IT or Academic Technology Personnel for additional information.

Messaging Technologies
Use of email and other messaging technologies shall not be used to transmit confidential or restricted information in an unencrypted format. Users must pay additional attention to email content and senders and must not open email attachments from unrecognized or suspicious senders. If there are questions about the security of an email message or email attachment, users should contact BCC IT Personnel.

Information Protection
In the course of performing their jobs, users may have access to confidential or proprietary information. Information is classified in the BCC Information Classification Policy. It is not permissible for users to acquire, or attempt to acquire access to confidential data unless such access is required by their jobs. Under no circumstances may users disseminate any confidential information, unless such dissemination is required by their jobs and explicitly approved.

Incident Response
BCC IT is tasked with responding to all IT-related security incidents such as computer virus infections. In order to effectively respond to these events IT relies on timely information and reporting from users. Consequently, users are required to contact IT or Campus Security, if:

- They observe suspicious activity
- They know or suspect that a security incident has or is going to occur

Passwords
Many BCC systems and applications require the use of a unique user identification and passwords. Unfortunately, due to the rising use and effectiveness of password guessing software tools and social engineering campaigns targeting users, it is important for BCC users to create, use, and protect strong passwords. To this end, users must never share their passwords with anyone else, and must promptly notify IT personnel if they suspect their passwords have been compromised.
IT Personnel will never ask for a user's passwords. Passwords must not be a single word or common phrase. All passwords must be at least eight characters in length and contain uppercase characters, lowercase characters, and numbers or symbols. Massachusetts Commonwealth and BCC systems require password changes every 90 to 180 days.

Physical and Environmental Security
Assistance from users is required to facilitate a physically and environmentally secure working environment. Users are required to be aware of locking and access restriction mechanisms and must proactively challenge, or alert IT or Campus Security if they are aware of unidentified or unescorted personnel within the premises. Additionally, to aid in the physical security of workstations and information technology resources, users who will be leaving their devices unattended for extended periods should log off before leaving. On all college systems, password protected screensaver applications should be set to automatically activate after no more than 15 minutes of inactivity.

Security Awareness Training
All BCC personnel are required to attend security awareness training upon hire and at least annually thereafter. Upon the completion of training, users will be required to provide acknowledgement that they have received and understand the training.

Unacceptable Use
Unacceptable uses of the College's ITRs, which will amount to a violation of this policy, will include, but not be limited to, the following:

- For any illegal act, including violation of any criminal or civil laws or regulations, whether state or federal;
- For any political purpose;
- For any commercial purpose;
- To send threatening or harassing messages, whether sexual or otherwise;
- To access, share or download sexually explicit or obscene material;
- To infringe any intellectual property rights, including copyright infringement;
- To gain, or attempt to gain, unauthorized access to any computer or network or information stored thereon;
- For any use that causes interference with or disruption of network users and resources, including propagation of computer viruses or other harmful programs;
- To intercept communications intended for other persons;
- To misrepresent either the College or a person's role at the College;
- To distribute chain letters;
- To access online gambling sites; or
- To libel or defame any person.

Additional examples of inappropriate use of the BCC electronic communications systems include, but are not limited to: excessive, unreasonable or unauthorized personal use; storing, sending or forwarding email messages that contain libelous, defamatory, racist, obscene, inappropriate, or harassing remarks; visiting or sending information to or receiving or downloading information from Internet sites involving inappropriate topics such as pornography, terrorism, violence, racism, or gambling.

Employees are prohibited from installing software onto BCC systems without prior approval from authorized IT personnel. Employees should not attempt to circumvent or disable protection mechanisms that have been put in place by BCC.

Enforcement
Any student, staff, or faculty member found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including suspension or termination of employment.

Violations
A user who violates this policy may be subject to civil and/or criminal liability for violating Commonwealth or federal laws, including, but not limited to: the Electronic Communications Privacy Act of 1986, the Family Educational Rights and Privacy Act (FERPA), Massachusetts Wiretap Law, defamation, copyright and/or trademark infringement laws, the Digital Millennium Act or sexual harassment or discrimination laws.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
CISO and Senior BCC Administration	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.
All Users, Students, Faculty, and Staff	Understand and adhere to this policy. Use BCC resources in only those methods, which have been identified as acceptable by this policy. Immediately report suspicious activities or violations of this policy to their manager or IT Personnel.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
DS5 Ensure System Security DS8 Manage Service Incidents	PCI Requirement 4: Encrypt transmission of cardholder data across open, public networks. Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs Requirement 8: Identify and authenticate access to system components. Requirement 12: Maintain a policy that addresses information security for all personnel. MA 201 CMR 17:00 Section 17.16 Section 17.20	

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	10/28/2015	Compass ITC	Initial Draft
1.1	6/15/2018		Revision
1.1.1	9/16/2019		Revision
1.1.3	11/1/2019		Revision
1.1.4	1/14/2020		Revision