Version: 1.2.3
Issued: 3/10/2020

Remote Access and VPN Policy – BCC02

PURPOSE

The purpose of this policy is to define the process and requirements for connecting to the Berkshire Community College (BCC) or using BCC technology to connect to other Commonwealth resources. These requirements are designed to minimize the potential exposure to damage, which may result from unauthorized use of institutional resources. Such damage may include the breach of sensitive or organizational information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system availability, or the corruption of information integrity.

SCOPE

This policy applies to all BCC employees, students, contractors, and third parties who access BCC applications, systems, or hardware remotely or use BCC resources to access other MA systems.

POLICY

All remote access to BCC applications, systems and hardware shall be authorized and approved. Any access not explicitly authorized and approved is forbidden. Remote access to specific applications, systems, components, and technology infrastructure shall only be granted to personnel with a legitimate need for such access. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

Employees and third parties authorized to use remote connections shall ensure that unauthorized users are not allowed access to the BCC internal network using these connections. All individuals and devices, accessing the network, including College owned and personal equipment, are a de facto extension of the College's network and, therefore, this equipment is subject to BCC's Information Security Policies.

All devices (and the networks they employ) that are connected to the BCC network or other Commonwealth resources via remote access technologies must use the most up-to-date antivirus software and be up-to-date on available system patches. This includes personal computers and LANs. Security patches for installed operating systems (with auto-update enabled), web browsers, and common applications shall be applied in a timely manner. A firewall must be installed and enabled on each applicable device and access may not be initiated from unsecured public or home networks.

Remote access services may only be used for conducting College related work. Personal, family, private, or commercial use of any service available remotely is not permitted.

Users agree to apply safeguards to protect BCC information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remotely accessed data or services, as well as prevention of inadvertent or intentional viewing of displayed information.

Remote access to data or services may not be used to copy private or personal information, such as that on College servers, shared files, or other College or Commonwealth information systems.

ENFORCEMENT

Any employee found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including termination of employment, as determined through Human Resources.

I, the undersigned, have read, understand, and agree to comply with the BCC Remote Access Policy governing the use of the remote access privileges assigned to me. Use of his access may be routinely monitored and will be terminated if there is evidence of misuse.

Print Name: **Sign:** **Date:**

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Director of Information Technology/CISO	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.
IT Staff	Ensure that individuals assigned to remotely access their applications are authorized and assigned duties that require these access capabilities. Ensure that the IT infrastructure is protected against unauthorized remote access. Administer the setup of newly added devices to be used for remote access.
Management Team	Determine which employees need remote access to their resources.
All Users	Understand and adhere to this policy. Safeguard their user IDs and passwords. Immediately report suspected violations of this policy to their supervisor or the Director of Information Technology.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
DS5.3 Identity Management DS5.4 User Account Management	PCI Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 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 17.04	

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
1.2	1/10/2020		Update
1.2.1	2/4/2020		Update
1.2.2	3/10/2020		Signature Requirement