SECTION: General Administrative | BCOM Policy 2010

TOPIC: Data Security Policy | Approval Date: 02/23/17

Effective Date: 02/23/17

Approved: *Signature on File* |

PURPOSE

BCOM aspires to provide responsible use and management of its technology resources including storage and use of confidential or protected data.

SCOPE

The administration shall establish rules and processes to secure and protect such protected data and shall establish such administrative, technical, and physical safeguards as may be necessary or appropriate to comply with all relevant data protection laws and contractual requirements. BCOM shall identify an IT security authority to monitor and report data security risks to the administration, address any data security breaches as required by law and BCOM rules, and to serve as a resource to the college community for data security and regulatory requirements.

RESPONSIBLE OFFICIAL(S):

The Responsible Policy Official(s) for this policy include the Chief Information Officer (CIO), and any employee specifically delegated by this individual to oversee the development and administration of the policy.

DEFINITIONS

“Confidential Data” is a generalized term, and not as a data classification.

POLICY

BCOM utilizes several software systems to manage a variety of student, staff, and corporate information. System security and integrity is a core requirement for all systems. There are several overall design requirements for BCOM software systems.

1) All systems will have integrated security features, including complex passwords and password encryption in transit and at rest.
2) All systems will allow for different levels of access to be granted to individuals as appropriate.
3) Data should be sent between servers and clients using industry standard encryption protocols.
4) All employees and students agree to the BCOM Acceptable Use Policy which describes ways to protect their systems and passwords from unauthorized disclosure or “hacking” attempts.
5) The BCOM Policy on Personnel/Student Personal Information/Records describes specific additional requirements for student and medical record protection.
6) Where possible, a separation of account management, and system operation is made. This is particularly true for financial and student record systems. This prevents operational users from changing their own access levels and enforcing access to those levels that are approved.

There are several broad categories of systems at BCOM, and each has different password requirements:

1) Student Information Systems (Primarily CAMS)
    a. Accounts are requested / authorized by the Associate Dean for Admissions and Student Affairs
    b. Accounts are limited to specific areas of the system as appropriate for the job function. For example, some personnel may be authorized to update student demographic information, while others have read only or no access.
    c. Accounts are provisioned by the CIO. Operational users cannot add or modify account access for themselves or others.

2) Business Operations (Primarily Dynamics GP)
    a. Accounts are requested / authorized by the VP for Administration/CFO.
    b. Accounts are limited to specific areas of the system as appropriate for the job function. For example, some personnel may be authorized for human resource record update, while others have read only or no access.
    c. Accounts are provisioned by the CIO. Operational users cannot add or modify account access for themselves or others.

3) Instructional Support (Primarily Canvas/Panopto/ExamSoft)
    a. Standard access is provisioned automatically for students and staff
    b. Access levels for Course Directors is assigned based on class schedules / assignments
    c. Additional elevated privileges may be authorized at the Associate Dean level or above.
    d. Management access is limited to IT Department and Instructional Specialists

4) Network / Systems Operations
    a. These are systems that provide configuration and control of the network environment, including WiFi, shared drive access, server management, and Internet control
    b. Accounts are limited to IT staff and/or 3rd party management providers as authorized by the CIO.
    c. This access level does NOT have the ability to create / modify users for areas 1 & 2 above.

5) Building Operations / Security
    a. These are systems that allow for building operations, safety, and security. These would include video surveillance systems, energy management, key card access control, and emergency notification.
    b. Access and level is authorized by the CIO
    c. Accounts are limited to specific areas of the system as appropriate for the job function. For example, some personnel may be authorized monitor video surveillance, but not to view recordings or download content.

6) General student and staff accounts
    a. This category created the basic login credentials for all students and staff.
    b. Typical access in this category is email, printing, computer login, and shared drives.
    c. These accounts are created automatically
    d. Privilege levels are assigned in broad groups. E.g. Staff would have broader shared drive access than students.