BRIDGEVALLEY COMMUNITY AND TECHNICAL COLLEGE

OPERATING POLICY

Effective Date	Subject	Number	Page
September 24, 2014	**BANNER ACCOUNTS**	B-OP-19-14	1 of 5
Supersedes/Supplements:	BC A-OP-2-12		
Reference:	None		

POLICY STATEMENT

To ensure confidentiality and appropriate use of student data, BridgeValley Community and Technical College (College) is dedicated to maintaining necessary security levels for data housed in the Banner Information System. Access rights to Banner data will be determined on a need-to-know basis through the Chief Banner Systems Officer (CBSO). Employees who are provided access will be required to sign a Code of Responsibility for Security and Confidentiality of Records and Files (CRSCRF) form.

PROCEDURES

To get a Banner account created or to request additional Banner rights, a Banner Account Request (BAR) form must be filled out by the user and approved by the supervisor. The form can be requested from the CBSO or via SharePoint as an attachment to this policy. Once the form has been completed, it must be signed by the user's supervisor and returned to the CBSO.

The request will be reviewed and the data owners for the screens being requested will be contacted for their approval. Upon their approval, the screens will be added to the user's accounts. Accounts will be created or modified up to five (5) days after approval. Once the account is created, the CBSO will provide the username and password to the user.

All Banner users will be required to sign the CRSCRF form concerning student data.

Banner accounts will be reviewed on a yearly basis to determine access needs.

Banner users will be required to attend one Banner training class a year.

Repeated attempts to access screens not authorized for use will result in the following:

First offense - Verbal warning from Student Systems
Second offense - Written warning from Student Systems
Third offense - Notification to user's supervisor
Fourth offense - Account locked and President notified

Faculty and Student access to Banner system will be via Self Service Banner.

Human Recourses will notify the CBSO of any change in a user's employment status so appropriate action may be taken to secure the user's account.

If a user's account becomes locked for any reason, the user must contact the CBSO.

PASSWORD STANDARDS

- Internet Native Banner (INB) users
    - The lifetime of the password is 60 days.
    - The password cannot be the same as the username (the user's id on the database).
    - The password must be at least eight (8) characters.
    - The user must wait one (1) hour between password changes.
    - There's a list of 'unallowed' passwords (like 'password' and '12345678'). See Appendix A.
    - Password must contain at least one digit and one character.
    - Password must differ by at least three (3) characters from the previous password.
    - Three (3) failed login attempts in a row will lock up the id; it is locked for one (1) hour.
    - An old password can never be reused; the database keeps the last three (3) passwords to check against.
    - The grace period for an expired password is seven (7) days.

- Self Service Banner (SSB) user
    - The password must be at least six (6) characters.
    - New passwords or reset passwords will be set to pre-expire and require user to create a new password.
    - Passwords cannot be reused.
    - Users will be required to have two security questions, which can be used for password recovery or user identification.
    - Passwords will expire 365 days after being changed.

DEFINITIONS

Chief Banner Systems Officer – CBSO

Code of Responsibility for Security and Confidentiality of Records and Files – CRSCRF

Banner Account Request – BAR

Internet Native Banner - INB

Self Service Banner - SSB

Approved by: Cabinet **Date:** 9/24/2014

Last Name _____ **First Name**_____
(Please Print)

BridgeValley Banner

Code of Responsibility for Security and Confidentiality of Records and Files (CRSCRF)

Security, confidentiality, and the appropriate use of your account are matters of concern to BridgeValley Community and Technical College (College). The purpose of this Code is to clarify employees' responsibilities regarding the use of your account when utilizing student records and files. Since conduct either on or off the job could affect or threaten the security and confidentiality of this information, each employee is expected to adhere to the following:

1. Account utilization outside normal College business hours and from outside the College campus network will be monitored.

2. Employees are not permitted to change data for themselves, friends or family members.

3. Employees are expected to maintain a clear understanding of the types of information that can be released without the student's consent. Questions as to dissemination or use of student data should be directed to the office of the Registrar.

4. Accounts may have access to personal or confidential information. This information is to be used for business purposes only. Employees may not seek personal benefit or allow others to benefit personally by knowledge of any confidential information that has come to them by virtue of their Student Information System access.

5. Employees may not exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and in accordance with College policies and procedures. Releasing any data or misuse of the data may be a violation of federal and/or state law, as well as the Family Educational Rights and Privacy Act of 1974 (FERPA).

6. No official record or report, or copy thereof, may be removed from the office where it is maintained, except in the performance of an employee's official duties. Reports must be stored in a secure area out of public view.

7. The account provided to BANNER System users is to be utilized by the owner only. **DO NOT SHARE ACCOUNTS**. Your account is confidential.

8. Access to BANNER is for business purposes only. Although the employee may have the ability to access information for units other than the campus, college, school, or departments for which they are responsible, the employee will not access or maintain, without prior approval, the information for any other college, school, or department.

9. Knowledge of a violation of this code by any individual must be immediately reported to that person's supervisor.

10. No employee is to aid, abet, or act in conspiracy with another to violate any part of this code. **Any breach of the violation of the Code of Responsibility may lead to reprimand, suspension, dismissal from the job or other civil and/or criminal penalties.**

I have read the above Code of Responsibility for Security and Confidentiality of Records and Files. I understand the intent and specific requirements of the Code of Responsibility, and I hereby verify that I will comply with all parts of the Code of Responsibility.

Signature _____ Date _____

Banner Account Request (BAR)

Please do not request accounts for students

New Account _____ Modify Account _____ Delete Account _____

Last Name: _____ First Name:_____ MI:_____

Department: _____ Phone: _____

E-mail Address: _____

Title: _____

Modules/Forms Requested: _____

_____

_____

_____

_____

Authorization Signature

_____ _____

(Requestor's Name – Please Print) (Data Owner – Please Print)

_____ _____

(Requestor's Signature / Date) (Data Owner- Signature/Date)

Appendix A

Unallowed Passwords

welcome1
database1
account1
unknown1
unknown0
incorrect1
incorrect0
password
12345678

In addition, the password is not allowed to start with:

dat
pas
use
abc
hel
123