

BROWARD COMMUNITY COLLEGE

Credit Card Guidelines & Security Rules

The purpose of this agreement is to maintain rules and guidelines for use of credit card information in the Broward Community College computing environment. The Network Security Officer/System Administrators have the authority to disable logins immediately for failure to comply with this agreement. These rules apply to any systems on the BCC College wide Network.

Information Sensitivity

Personal information is defined as a combination of items 1 and 2:

1. First name (or first initial) and last name
2. Social Security Number, driver's license or identification card number, bank account or credit card numbers

Sensitive information is defined as any personal information items and includes:

- Usernames, passwords, credit card information, addresses, phone numbers, and email addresses.
- Sensitive information is not to be released unless prior written approval is received from the person whose information is in question.
- Sensitive information must be securely disposed of when no longer needed. Consult with your supervisor for specific disposal techniques for all sensitive information.
- The full contents of credit card magnetic stripes (or chips, or other storage mechanism) may not be stored in any database, log files, or point of sale products.
- The card-validation code may not be stored in any database, log file, or point of sale product.
- All but the last four digits of credit card account numbers must be masked (ie. with X's or *s) when displaying cardholder data.
- Credit card account numbers should never be sent over e-mail.
- The only personnel who should have access to customer sensitive information are those with explicit need-to-know.
- Sensitive information printed on paper or received by fax must be protected against unauthorized access.
- **Security incidents should be immediately reported to the Information Security Officer. An incident response team will be appointed by the Information Security Officer, and will be ready for deployment in case of credit card data compromise.**

Acceptable Use

- All data contained on, or passing through BCC assets is subject to monitoring and remains the property of the college.
- Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing BCC-owned resources.
- Employees who receive a username and password must keep that information confidential and not allow use of their account by others.
- Employees who leave their workstations should enable a password protected screensaver or log off to prevent unauthorized access
- Employees must not use BCC network or email accounts to post publicly accessible messages or posts.
- Employees must not tamper with or disable anti-virus software installed on their workstations
- Employees are expressly forbidden to install any software on their workstations without prior approval from their supervisor
- Employees must be very careful when opening email attachments, and should disregard unsolicited emails containing attachments
- Employees may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to elevate privileges or gain access to information that was not expressly intended for them
- Employees must not reveal any information about BCC students, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission from their supervisor.
- Employees must not use their BCC email accounts for purposes other than the conduct of BCC business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes.

Disciplinary Action

Failure to comply with this security policy may result in disciplinary action up to and including termination of employment.

USER ACCEPTANCE:

By signing this form, I have read and I clearly understand my responsibility and will abide by the above terms and condition of the Credit Card Guidelines and Security Rules for use of these facilities. I acknowledge receipt this date of a written copy of this form. If the propriety of any situation is unclear, I will ask for clarification from my supervisor rather than making any assumptions.

_____/____/____
Employee Signature Date

Printed Name

Dept Name

Date

(954) 201 - _____