# BUFFALO STATE COLLEGE

## DIRECTORY OF POLICY STATEMENTS

Policy Number: VI:21:01 Date: November 2008

**Subject: Maintaining the Security, Confidentiality, and Integrity of Customer Information**

In compliance with the *Gramm-Leach-Bliley Act* and the rules promulgated therein by the Federal Trade Commission, Buffalo State College requires that all employees receive the following guidelines to ensure the security and confidentiality of customer records and information:

Control access to rooms and file cabinets where paper records are kept:

- All doors to office areas must be locked during non-business hours.
- Work areas where customer information is processed must be behind locked doors or otherwise secured during business hours.
- Guests should be escorted in areas where customer information is being processed.
- Guests should be restricted to areas that do not have customer information in plain view. Conversely, customer information should be kept out of areas accessible to students and the public.
- File cabinets used to store customer information must be secured in locked areas.
- Fireproof cabinets used to store promissory notes must be locked during non-business hours.
- Records containing customer information are to be retained only as long as they are valid, useful, and required to be retained. When no longer needed, paper, microfilm, and microfiche records must be destroyed by shredding. Electronic records must be destroyed according to current guidelines available from Computing Services and Facilities Office.

Control access to information stored electronically:

- Workstations should be behind locked doors or otherwise secured.
- Employees should “minimize” any computer windows not in use, to prevent inadvertent breaches.
- Employees are encouraged to password-protect their workstations when not in use.
- Employees should use strong passwords for all systems (at least eight characters, alphanumeric).
- Employees should change their passwords every 60 days or less.

- Employees must not post passwords on or near their computers.

- Access to student and employee records systems will be granted only to those employees whose job duties require them to access customer information.

Protect our customer's information:

- Employees should respond to requests for customer information in accordance with the *Family Educational Rights and Privacy Act* (FERPA). FERPA questions or potential violations should be referred to the Registrar's Office.

- Employees should refer to appropriate security policies as needed to ensure compliance.

- Employees must report any fraudulent attempt to obtain customer information to management, who should then report the attempt to the Vice President for Finance and Management's Office.