Identity Theft Prevention Program for State University College at Delhi

This Identity Theft Prevention Program ("Program") was developed pursuant to a SUNY policy adopted by the Board of Trustees on May 12, 2009 in order to comply with the Federal Trade Commission's Red Flags Rule (16 CFR 681.2). The purpose of this Program is to prevent frauds committed by the misuse of identifying information (i.e. identity theft). The Program aims to accomplish this goal by identifying accounts maintained by the College which may be susceptible to fraud (hereinafter "Covered Accounts"), identify possible indications of identity theft activityassociated with those accounts (hereinafter "Red Flags"), devising methods todetect such activity, and responding appropriately when such activity is detected.

Definitions:

Account:	A relationship established with an institution by a student, employee, or other person to obtain educational, medical, or financial services.
Covered Account:	An account that permits multiple transactions or poses a reasonably foreseeable risk of being used to promote an identity theft.
Responsible Staff:	Personnel who regularly work with Covered Accounts and are responsible for performing the day-to-day application of the Program to a specific Covered Account by detecting and responding to Red Flags.
Red Flag:	A pattern, practice, or specific activity that indicates the possible existence of identity theft.
Response:	Action taken by Responsible Staff member(s) upon the detection of any Red Flag to prevent and mitigate identity theft.
Service Provider:	A contractor to the College engaged to perform an activity in connection with a Covered Account.
Identity Theft:	A fraud committed or attempted using the identifying information of another person without authority.

Program Administration and Oversight:

The President has designated the Vice President for Business & Finance as Program Administrator to oversee administration of this Program. The Program Administrator may designate additional staff of the College to undertake responsibility for training personnel, monitoring service providers, and updating the Program, all under the supervision of the Program Adminstrator.

The Program Administrator or designees shall identify and train responsible staff, as necessary, to effectively implement and apply the Program. All College personnel are expected to assist the Program Administrator in implementing and maintaining the Program.

The Program Administrator or designees shall review service provider agreements and monitor service providers, where applicable, to ensure that such providers have adequate identity theft prevention programs in place. When the Program Administrator determines that a service provider is not adequately guarding against threats of identity theft, he/she shall have the authority to take necessary corrective action, including termination of the service provider's relationship with the College.

Prior to the beginning of each academic year, the Program Administrator shall evaluate the Program to determine whether it is functioning adequately. This evaluation shall include: a case-by-case assessment of incidents of identity theft or attempted identity theft that occurred during the previous academic year; interviews with Responsible Staff; and a survey of all accounts maintained by the College to identify any additional Covered Accounts. In response to this annual evaluation, the Program Administrator shall recommend amendments to this Program for approval by the President.

The Program Administrator shall maintain records relevant to the Program, including: the Written Program; documentation on training; documentation on instances of identity theft and attempted identity theft; contracts with service providers that perform activities related to Covered Accounts; and updates to the Written Program. From time to time, the College Vice President for Business & Finance, or other designated internal control officer, may perform audits to determine if various segments of the College are in compliance with the Program.

Covered Accounts; Responsible Staff; Red Flags; Responses:

Covered Account: **Student Accounts**

Responsible Staff: Cashiers

Background: Students must present college identification card or valid driver's license with picture when signing over a loan check to go on their account.

Red Flag 1:	Student does not have ID card.
Response:	Do not allow student to sign check over. Make student return with ID card or driver's license.

Covered Account:	**Student Refund Checks**
Responsible Staff:	Student mailroom staff
Background:	All refund checks are sent to the student mailroom and put in student's individual mailbox. Each student is assigned a mailbox and given a combination.
Red Flag 1:	Student forgot combination.
Response:	Staff will require student to present ID card for identification and give student combination.

Covered account:	**Employee Paychecks**
Responsible Staff:	HR staff
Background:	Staff paychecks and direct deposit stubs are distributed by Human Resources' staff and other staff bi-weekly
Red Flag 1:	An unknown staff member requests a paycheck
Response:	Do not issue check without valid identification.
Red Flag 2:	A co-worker, spouse, domestic partner or other party asks for an employee's check
Response:	Do not issue check without written confirmation from the employee.

Covered Account:	**Employee payroll and personnel records**
Responsible staff:	HR staff
Background:	Employees provide personal information for payroll and benefits. Information is stored in electronic and paper formats.
Red Flag 1:	Employee provides conflicting information (e.g. more than one social security number).

Response:	Investigate discrepancies before proceeding with processing of payroll and benefits.
Red Flag 2:	Employee reports identity theft which appears to be tied to employment/payroll records.
Response:	Gather information and investigate in concert with SUNY Counsel and external agencies which manage HRIS (SUNY University Wide Human Resources, Civil Service, NYSHIP)

Covered Account:	**Bronco Web (Banner Self-Service via Web)**
Responsible Staff:	Computer Information Systems (CIS)
Background:	Students are automatically assigned a username and password to access their student records via web using Banner Self-Service.
Red Flag 1:	The student notifies CIS's Client Support Services' Help Desk that he or she believes that someone else has gained access to his or her student record via Banner Self-Service.
Response:	Notify student that he or she should change his/her password. If student does not want to change his/her own password, have student contact the Office of the Registrar. If student provides proper identification, in person, the Office of the Registrar will reset password. If student provides sufficient identification over the telephone, Office of the Registrar will cause a new password to be mailed to the student's permanent address on file.
Red Flag 2:	A college office notifies CIS's Client Support Services' Help Desk that it appears someone else has gained access to records of a student via Banner Self-Service.
Response:	CIS's Client Support Services' Help Desk will investigate. If CIS agrees that this is a reasonable assumption, CIS Client Support Services' Help Desk will disable the student's pin/password to prevent further unauthorized access. The student will need to be provided with a new password before computer access may be restored.

Covered Account:	**Student E-mail**
Responsible Staff:	Computer Information Systems (CIS)

Red Flag 1: The student notifies CIS's Client Support Services' Help Desk that he or she believes someone else has gained access to his/her college e-mail account.

Response: Notify student that he or she should change his/her password. If student does not want to change his/her own password, CIS's Client Support Services' Help Desk will reset password and provide the student with the new password.

Red Flag 2: A college office notifies CIS's Client Support Services' Help Desk that it appears someone else has gained access to a student's e-mail account.

Response: CIS's Client Support Services' Help Desk will investigate. If CIS agrees that this is a reasonable assumption, CIS's Client Support Services' Help Desk will reset password to prevent further unauthorized access. The student will be provided with the new password.

Covered Account: **Employee Bronco Web (Banner Self-Service via Web)**

Responsible Staff: Computer Information Systems (CIS)

Background: Employees are assigned a username and password to access their own records and records of students via web using Banner Self-Service.

Red Flag 1: The employee notifies CIS's Client Support Services' Help Desk that he or she believes that someone else has gained access to his/her records via Banner Self-Service by using his/her username/password.

Response: CIS's Client Support Services' Help Desk will reset password and provide it to the employee.

Red Flag 2: A college office notifies CIS's Client Support Services' Help Desk that it appears someone else has gained access to records via Banner Self-Service using a username/password assigned to an employee.

Response: CIS's Client Support Services' Help Desk will investigate. If CIS agrees that this is a reasonable assumption, CIS's Client Support Services' Help Desk will disable the employee's pin/password to prevent further unauthorized access. The employee will need to be provided with a new password before computer access can be restored.

Covered Account: **Employee E-mail**

Responsible Staff: Computer Information Systems (CIS)

Red Flag 1: The employee notifies CIS's Client Support Services' Help Desk that he or she believes someone else has gained access to his/her college e-mail account.

Response: CIS's Client Support Services' Help Desk will reset password and provide the new password to the employee.

Red Flag 2: A college office notifies CIS's Client Support Services' Help Desk that it appears someone else has gained access to an employee's e-mail account.

Response: CIS's Client Support Services' Help Desk will investigate. If CIS agrees that this is a reasonable assumption, CIS's Client Support Services' Help Desk will reset the employee's password to prevent further unauthorized access and provide the new password to the employee.

Covered Account: **Student Record**

Responsible Staff: Registrar's office staff

Background: A student may change his/her temporary or local address online in Bronco Web but they cannot change the permanent address in the Banner computer system. To change the permanent address, the request must be made in writing to the Registrar's office.

Red Flag 1: A student calls or e-mails a change of address request.

Response: If a student or parent calls over the phone they will be asked to have the student stop by the Registrar's office to put the request in writing. If the request comes from a non-student e-mail account such as G-mail or Yahoo, the registrar's office staff will ask the student to come to the office or put it in writing with a signature before changing the address. If the request comes from the student's Delhi e-mail address the address will be changed.

Red Flag 2: A change of name request occurs without appropriate identification and/or documentation.

Response: Deny name change request until student's identity has been established through acceptable means and/or appropriate documentation is provided.

Covered Account: **Financial Aid Grant and Loan Accounts**

Responsible Staff: Financial Aid Staff

Red Flag 1:	U.S. Department of Education selects student's FAFSA for verification.
Response:	Collect supplemental information from student and resolve any conflict between FAFSA and supplemental information provided by student.
Red Flag 2:	Student submits multiple FAFSAs containing conflicting information.
Response:	Contact student to resolve conflict and verify information.
Red Flag 3:	Personal identifying information provided with the loan application is not consistent with other personal identifying information on file.
Response:	Ask applicant for additional information to verify applicant's identity and/or resolve any discrepancies with identifying information on file.