Suffolk County Community College
Identity Theft Prevention Program

This Identity Theft Prevention Program was developed 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 (Covered Accounts), identifying possible indications of identity theft activity associated with those accounts (Red Flags), devising methods to detect such activity, and responding appropriately when such activity is detected.

I. 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, based on title, 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.

II. Program Administration and Oversight

The President has designated the Executive Director for College Safety and Security Compliance 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 Administrator.

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 the following: 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, if necessary, recommend amendments to this Program for approval by the Board of Trustees.

The Program Administrator shall maintain records relevant to the Program, including the following: 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 Vice President for Business and Financial Affairs, or other designated College official, may perform audits to determine if various segments of the College are in compliance with the Program.

III. Covered Accounts; Responsible Staff; Red Flags; Responses:

Covered Account:	Student Accounts
Responsible Staff:	Student Services Representatives
Red Flag 1:	Suspicious ID presented by a student who is trying to access or alter account.
Response:	Deny access to account until the student's identity has been established through acceptable means.
Red Flag 2:	A change of address request occurs under suspicious circumstances.
Response:	Ask student to come in and personally verify address and any suspicious usage activity.

Covered Account:	Financial Aid Account
Responsible Staff:	Financial Aid Advisors
Red Flag 1:	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:	The National Student Loan Data System (NSLDS) indicates that a student has one or more student loans in a status associated with identity theft.
Response:	College financial aid advisor provides NSLDS with requested information and awaits notification from NSLDS that issue has been resolved. No aid is awarded until resolution.
Red Flag 4:	NSLDS indicates that a student has one or more student loans that may have been obtained fraudulently.
Response:	Student is instructed to contact NSLDS directly. No aid is awarded until the College is notified by NSLDS that it can process aid.

Covered Account:	Email Accounts
Responsible Staff:	Information Technology
Red Flag:	Students reports attempts or unauthorized access to their portal and/or email accounts to the Campus Registrar's office
Response(s):	Once the individual's identity has been verified by the Registrar's office, the student's password will be reset. In addition, the Computer Center will review available log activity on the account see if the attempts or unauthorized access can be identified. If necessary, a new account will be generated for the student.

Covered Account:	Banner Accounts (Employees with Access to Student Records)
Responsible Staff:	Computer Center Security Officer
Red Flag:	After multiple failed login attempts, Banner will automatically lock access to an individual's account.
Response:	Locked accounts will be reviewed and logged. These will remain frozen until the account owner reports the lock. The Computer Center will verify that the owner initiated the lock and unfreeze the account. If there is a

question as to who caused the lock, the Computer Center will unfreeze and log attempts to the account and initiate procedures to verify who is attempting to access the account.

Covered Account:	Emergency Loans
Responsible Staff:	Campus Business Officers and Financial Aid Advisors
Red Flag:	Suspicious ID presented by a student who is trying to access emergency loan funds.
Response:	Deny access to emergency loan funds until the student's identity has been established through acceptable means.

Board of Trustees Adopted
October 22, 2009