

# NORTHWOOD TECHNICAL COLLEGE



## ADMINISTRATIVE PROCEDURE: J-115A

### TITLE: Red Flag Rule - Student Identity Theft Prevention Procedure

#### CROSS-REFERENCE(S):

Technology Acceptable Use Handbook

#### A. PURPOSE AND APPLICABILITY:

To comply with Section 114 of the Federal Trade Commission's Fair and Accurate Credit Transactions Act of 2003 - *Red Flags* Rule. This regulation requires Northwood Technical College (College) to have an Identity Theft Prevention Program designed to detect, prevent, and mitigate Identity Theft in connection with opening a covered account or existing covered account and to provide administration of the program.

#### B. PROCEDURE TO ENSURE STUDENT IDENTITY

To ensure compliance with the Red Flag Rule, College staff will verify student identity when fulfilling information requests. These requests can be, but are not limited to, any of the following services:

##### ITEMS REQUIRING STUDENT IDENTIFICATION

1. Student Admissions Information including test results
2. Student Record Information including schedules, transcripts, grades, etc.
3. Student Account information including billing inquiries, balance owed, authorizations, etc.
4. Student Financial Aid Information
5. Parking Permits
6. Student ID Cards or ID Badge
7. ANY OTHER INFORMATION OR DOCUMENT REQUIRING STUDENT ACCOUNT ACCESS

##### FORMS OF ACCEPTABLE ID

1. "One" Form of Photo ID:
  - a. Student ID
  - b. Driver's License
  - c. Passport
  - d. DMV Authorized ID Card
2. OR "Two" of the following may be used in place of a photo ID:
  - a. Social Security Card
  - b. Birth Certificate
  - c. Utility Bill
3. OR "Three" of the following presented verbally or in writing:
  - a. Student ID Number
  - b. Last 4 Digits of Social Security Number
  - c. Month and Day of Birth
  - d. Address on File
  - e. Last 4 Digits of Phone Number on File

#### C. PROCEDURE FOR REPORTING SUSPECTED OR REPORTED RED FLAG ISSUES

When a case of identity theft is reported or suspected, College staff members should do the following:

1. Staff Member should immediately report incident or suspicion to the campus Manager of Enrollment Services.
2. Manager of Enrollment Services and staff member should document the facts and immediately inform the VP of Student Affairs with the specific details.
3. The VP of Student Affairs, in consultation with the Red Flag Response Team, will determine necessary action as outlined in the Northwood Technical College Identity Theft Prevention policy.

#### **D. Appendix A - Training Handout for Staff**

##### ***GUIDELINES FOR KEEPING STUDENT INFORMATION CONFIDENTIAL***

To reduce the risk of identity theft, College staff members should practice the following:

1. Never ask a student to instant message or e-mail credit card information
2. Never ask a student to verbally declare their personal information in the presence of others
3. Don't leave documents containing sensitive information lying around
4. Shred or destroy sensitive personal documents before tossing them into the garbage or recycling

##### ***RED FLAGS FOR COVERED ACCOUNTS***

Northwood Technical College staff members should use the following risk factors to identify relevant red flags for covered accounts:

###### Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic
- The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification
- A request for service that appears to have been altered or forged
- A request made from a non-college issued e-mail account
- A request to mail something to an address not listed on the file

###### Suspicious Identifying Information

- Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates)
- Identifying information presented that is inconsistent with other sources of information (example: address mismatch on personal documents)
- Identifying information presented that is the same information shown on other applications that were found to be fraudulent
- Identifying information presented that is consistent with fraudulent activity (example: invalid phone number or fictitious billing address)
- Social security number presented that is the same as one given by another person
- A person fails to provide complete personal identifying information on a deferred payment plan when reminded to do so
- A person's identifying information is not consistent with the information that is on file for the student

###### Suspicious Account Activity

- Account used in a way that is not consistent with prior use
- Mail sent to the student is repeatedly returned as undeliverable
- Notice to the College that a student is not receiving mail sent by the College
- Notice to the College that an account has unauthorized activity
- Breach in the College's computer security system
- Unauthorized access to or use of student account information

###### Alerts from Others

Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

***Questions regarding this procedure should be directed to Student Affairs.***

Procedure Adopted: March 23, 2010

Procedure Revised: August 17, 2010

Procedure Reviewed: June 2, 2021

A handwritten signature in black ink, appearing to read "Joe Hill". The signature is written in a cursive style with a large initial "J".

---

PRESIDENT  
NORTHWOOD TECHNICAL COLLEGE