WGTC 3.27p

Identity Theft Prevention

This procedure establishes an Identity Theft Prevention Program for West Georgia Technical College to detect, prevent, and mitigate identity theft during the admission, financial aid awarding, or refund process for students at West Georgia Technical College. It is also to provide preventative measures against identity theft.

Definitions:

Identity Theft - fraud committed or attempted using the identifying information of another person without authority.

Red Flag - a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Identifying Information or Personal Identifying Information - any name or number used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license, government issued identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

Procedure:

Identification of Red Flags:

Suspicious Documents:

- Documentation that is not consistent with existing student information;
- Documentation used for identification that appears to be altered or inauthentic;
- Documentation used for identification with a photograph that is inconsistent with the person presenting the document.

Suspicious Personal Identifying Information:

- Inconsistent identifying information provided by student;
- Inconsistent identifying information between different sources;
- Identifying information given that has been previously found to be fraudulent;
- Identifying information given that is consistent with fraudulent activity;
- Identifying information such as social security number, address, or phone number that is the same as another student;

- Failure to provide the necessary personal identifying information when requested;
- The identifying information does not match the existing student records.

Suspicious Activity with Notification from BankMobile:

- BankMobile has its own policies to prevent identity theft from existing accounts:
  - Accounts require a password and a one-time passcode sent to a mobile phone associated with the account.
  - Fraud reminders within the BankMobile account interface
  - Display banner messaging on their website
- Should their monitoring detect an issue with an existing account, an email is sent to the college to notify them that a Fraud Risk has been identified. BankMobile closes the account, and the WGTC Business Office updates the student's Banner account to reflect the change, ensuring that checks are issued for any refunds sent in the future. Notification is provided to the Admissions and Financial Aid Offices to review all student documentation to ensure compliance with the policy.

Detection of Red Flags:

- As part of the enrollment process and per TCSG admissions policy, Admissions requires identifying information, suchas name, date of birth, academic transcripts, home address or other forms of identification. As such, Admissions collaborates with various stakeholders to take reasonable measures to validate the legitimacy of the documents submitted.
  - A driver's license is one way to verify a person's identity and establish their validity.
  - As a best practice, Admissions checks the Georgia Department of Driver Services to verify the legitimacy of the driver's license number. (This process does not provide an image of the actual driver's license).
  - If the Georgia drivers' license number is not recognized on the Georgia Department of Drivers Services database and is currently unexpired, we consult with the West Georgia Technical College Police Department.
  - Admissions uses the following criteria to review the license for authenticity:

Front of License:

1. The license contains too many pictures.
2. The date of birth (DOB) on the front does not match the DOB on the back.
3. The names of the Commissioner and Governor names are inconsistent with the year of issuance.
4. The picture displayed appears to be AI generated or photoshopped.
5. The "Star" in the top right corner is not black or gold.
6. The full signature is not located below the picture (in most states) and

does not appear to be original.
7. No county field provided.
8. Unrealistic physical characteristic data
9. Military emblems such as anchors, stars, and leaves appear on the driver's license.

Back of License:

1. The current license features an image displaying more than half of the Georgia Capitol Building.
2. The date of birth (DOB) aligned with the lower right corner.
3. The top barcode runs along the left side of the license, with the barcode number located at the bottom.

Academic Transcripts

1. The current mailing address reflected an out-of-state school.
2. Date of birth not in alignment with the normal graduation age, resulting in "aging out".
3. The cumulative GPA does not reflect honor listed on transcript, such as Magna Cum Laude.
4. The transcript contains personal comments about the student.
5. The school seal doesn't look authentic.
6. The general formatting of the transcript.

Business Office

- As part of the refund inquiry process, the Business Office will verify the identification of students if they request information regarding their accounts. The student must make all address and banking information changes after securely logging into the BankMobile site.

Prevention and Mitigation:

If a red flag is identified, one or more of the following actions will be taken, depending on the degree of risk, type of transaction, availability of contact information for the victim of fraud, and other factors:

- Apply codes in Banner that prevent refunds from being sent to BankMobile if the issue is with a compromised BankMobile account. The Business Office will issue a check and mail it to the student.
- Provide the student with a new student identification number.
- Notify the Information Technology department if student's account password needs to be reset or locked.
- Notify Campus Police.
- Notify the Financial Aid Office.
- Notify the Admissions Office.

To further protect student information and decrease the likelihood of Identity theft occurring, West Georgia Technical College has the following internal operating procedures:

- Office computers are password-protected.
- Multifactor Authentication (MFA) is implemented on faculty, staff, and student accounts.
- Secure destruction of paper documents and computer files containing student account information in compliance with the TCSG Retention Policy;
- When possible, avoid using social security numbers.
- Computer operating systems are patched, and endpoint protection is updated.
- Require and retain student information necessary for college operation purposes and to comply with the TCSG Retention Policy.

Staff Training:

West Georgia Technical College will send its policy regularly for staff to review. All faculty and staff are required to complete annual Security Awareness Training. Specific training will be provided for all employees working in Admissions, Financial Aid, and the Business Office, focusing on business practices and adherence to this policy.

Any identity theft incidents and the response to the incident will be reported immediately to the college President and TCSG Assistant Commissioner of Administration. Violations of these policies incur the same disciplinary measures as violations of other System or Technical College policies or state or federal laws, including criminal prosecution.

Reference: State Board Procedure 3.3.11p.
https://tcsg.atlassian.net/wiki/spaces/policymanual/overview

<table>
<tr><td>Policy Source: West Georgia Technical College</td><td colspan="2">Policy Manager: Vice President, Finance</td><td>Effective: 10/2025</td></tr>
<tr><td colspan="2">Division: Financial Services</td><td colspan="2">Reviewed:

Revised:</td></tr>
</table>