3357:13-13-061 Pre-Registration Fraud and Identity Verification Procedure

(A) General Process Standard

(1) North Central State College shall maintain a documented process for identifying, reviewing, communicating with, and resolving applicant identity verification or fraud concerns prior to registration.

(2) The process shall be risk-based, consistent, documented, and designed to protect legitimate students while preventing fraudulent applicants from gaining access to registration, financial aid, institutional systems, or student records.

(3) Applicants shall not be selected for enhanced identity verification based on personal characteristics, protected class status, assumptions, accent, name, national origin, disability, age, race, ethnicity, religion, sex, gender identity, veteran status, or other unrelated personal factors. Selection shall be based only on approved fraud-risk indicators, documentation concerns, system information, applicant behavior, or other objective criteria established through College procedure.

(B) Fraud-Risk Indicators

(1) The College shall maintain an internal list of approved fraud-risk indicators that may trigger additional review. These indicators may include, but are not limited to:

(a) Inconsistent or conflicting applicant identity information;

(b) Mismatch between application information and submitted documentation;

(c) Unusual geographic patterns inconsistent with the applicant's program, intended modality, or stated educational goal;

(d) Use of contact information, mailing addresses, phone numbers, IP/location information, or other data elements associated with known or suspected fraudulent activity;

(e) Multiple applications sharing common identifiers or suspiciously similar information;

(f) Unusual enrollment intent, especially where the selected program, course modality, distance from campus, or communication pattern does not reasonably align;

(g) Failure or refusal to provide requested identity documentation through approved secure methods;

(h) Submission of altered, unverifiable, suspicious, incomplete, or low-quality documentation;

(i) Application patterns associated with prior confirmed fraud attempts;

(j) Other documented concerns identified through Admissions, Financial Aid, Student Records, IT, Institutional Research/Information Systems, Advising, or other relevant offices.

(2) In general, an applicant shall be referred for enhanced review when two or more established risk indicators are present. A single risk indicator may result in enhanced review only when the concern is significant, directly tied to identity integrity, or connected to known fraud activity.

(C) Initial Identification

(1) Potential fraud or identity concerns may be identified by any office involved in the applicant intake, onboarding, financial aid, registration, advising, technology access, or records process.

(2) When an employee identifies a potential concern, the concern shall be referred through the College's designated fraud review channel. The referral should include, when available:

(a) Applicant name and College ID number, if assigned;

(b) Date the concern was identified;

(c) Office or employee submitting the referral;

(d) Specific risk indicators observed;

(e) Relevant screenshots, documents, notes, communication records, or system information;

(f) Whether the applicant is attempting to register, receive aid, access systems, or complete another time-sensitive action;

(g) Any immediate recommendation, such as temporary registration hold, additional documentation request, or cross-office review.

(3) Employees should avoid informal side-channel determinations. Concerns should be documented through the approved process so that the College can respond consistently and preserve an appropriate record of review.

(D) Temporary Registration or Processing Hold

(1) When an applicant meets the criteria for enhanced review, the College may place a temporary registration, admissions processing, account access, financial aid, or related administrative hold as appropriate.

(2) The purpose of the hold is not disciplinary. The purpose is to prevent further enrollment activity until the applicant's identity or legitimacy can be reasonably verified.

(3) Any hold used under this policy shall be:

(a) Narrowly applied;

(b) Documented in the appropriate system;

(c) Communicated internally to relevant offices;

(d) Reviewed in a timely manner;

(e) Removed promptly once the concern is resolved.

(4) The College shall establish internal procedures identifying which offices may apply or request holds, which systems shall be used, what language shall appear on the hold, and who has authority to remove the hold. Final authority for denying registration, closing or inactivating an application, determining that an applicant is unable to verify identity, or referring a matter for external reporting shall rest with the designated institutional official or review body identified in procedure.

(E) Applicant Communication

(1) Applicants selected for enhanced verification shall receive clear, respectful communication explaining that additional identity verification is required before registration or further processing may continue.

(2) The communication should state that verification is used to protect student identity, academic records, financial aid eligibility, and institutional resources. It should not accuse the applicant of fraud unless a formal determination has been made.

(3) Communication should include:

(1) What action the applicant must complete;

(2) The deadline for response;

(3) Approved methods for submitting or presenting documentation;

(4) A warning not to submit sensitive identity documents by unsecured email;

(5) Contact information for assistance;

(6) Notice that failure to complete verification may delay or prevent registration;

(7) A brief explanation that the process is part of the College's responsibility to protect students and institutional integrity.

(4) Where possible, the College should use consistent template language to avoid variation in tone, detail, or treatment between applicants.

(F) Verification Methods

(1) The College may use one or more approved methods to verify applicant identity. Verification methods may include:

(a) In-person presentation of government-issued photo identification;

(b) Secure upload of government-issued photo identification through an approved system;

(c) Live interaction with trained College staff using an approved identity verification protocol;

(d) Third-party identity verification service, if adopted by the College;

(e) Verification of official documents through issuing agencies or approved evaluators;

(f) Comparison of applicant information against internal records, known fraud indicators, or other authorized data sources;

(g) Other methods approved by the College and consistent with applicable law and policy.

(2) For higher-risk cases, in-person verification or another stronger verification method may be required. Remote or video-based verification may be used only when the College determines that the method is sufficient for the level of concern identified.

(3) The College shall not request or accept sensitive identity documentation through unsecured email unless no other method is available and the applicant has been informed of the risks and provided an alternative whenever possible.

(G) Review and Decision

(1) Enhanced verification reviews shall be conducted by designated staff or a designated review group according to internal procedure.

(2) The review may result in one of the following outcomes:

(a) Cleared: The applicant successfully verifies identity or resolves the concern. Holds are removed, and normal processing may continue.

(b) Pending Applicant Response: The applicant has been contacted but has not yet provided the required information.

(c) Additional Review Needed: The applicant's response is incomplete, inconsistent, suspicious, or requires review by another office.

(d) Unable to Verify: The applicant fails to complete verification, provides insufficient information, or cannot be reasonably verified.

(e) Confirmed or Substantiated Fraud Concern: The College determines that the applicant has submitted false, altered, stolen, misleading, or fraudulent information.

(3) The College shall document the basis for the decision, including the indicators reviewed, verification steps completed, applicant communication, offices consulted, and final outcome.

(H) Consequences of Failure to Verify

(1) If an applicant does not complete required verification by the stated deadline, the College may delay or deny registration, withhold further processing, close or inactivate the application, block account access, or take other administrative action consistent with College procedure.

(2) If the College determines that an applicant submitted fraudulent, altered, stolen, or intentionally misleading information, the College may deny admission, prevent registration, cancel pending enrollment activity, restrict system access, refer the matter to appropriate internal offices, or report the concern to external agencies when required or appropriate.

(3) Any action taken shall be documented and based on the available evidence.

(I) Cross-Office Coordination

(1) Fraud prevention requires coordinated review across offices. Internal procedures shall identify when and how concerns are shared among Admissions, Student Records, Financial Aid, IT, Institutional Research/Information Systems, Advising, Business Office, Academic Affairs, Campus Safety, and other relevant offices.

(2) Information sharing shall be limited to employees with a legitimate educational or institutional need to know. The College shall handle applicant information, identity documents, and fraud-review records in accordance with applicable privacy, records retention, data security, and FERPA-related requirements.

(J) Documentation and Recordkeeping

(1) The College shall maintain records of fraud-risk referrals, verification requests, applicant responses, review notes, decisions, and final outcomes according to institutional recordkeeping procedures.

(2) Documentation should be sufficient to show:

(a) Why the applicant was selected for enhanced review;

(b) What information was requested;

(c) How the applicant responded;

(d) Which offices participated in the review;

(e) What decision was made;

(f) When holds were applied or removed;

(g) Whether any further action or reporting occurred.

(3) Fraud-review records shall be stored securely and accessed only by employees with a legitimate need to review the information.

(K) Procedure Review and Continuous Improvement

(1) The Fraud Taskforce, or other designated College body, shall review fraud-risk indicators, verification methods, referral patterns, outcomes, and procedure effectiveness on a regular basis.

(2) The review should consider:

(a) Whether the indicators are identifying legitimate risk;

(b) Whether legitimate students are experiencing unnecessary burden;

(c) Whether fraudulent applicants are being stopped before registration;

(d) Whether communication templates remain clear and respectful;

(e) Whether additional staff training is needed;

(f) Whether system changes, software tools, or reporting improvements are needed;

(g) Whether state, federal, financial aid, cybersecurity, or higher education fraud guidance has changed.

(3) The College may revise procedures as needed to respond to emerging fraud patterns, technology changes, legal requirements, institutional risk, and student experience.

Effective: August 25, 2026
Next Review: August 1, 2031
Review Dates: 8/25/26