



National Intelligence University

POLICY MEMORANDUM

Policy No: NIU-1025.04

Date: 15 May 2013

Subject: Identity Verification Policy and Procedures

POLICY

1. **Purpose.** This memorandum documents National Intelligence University (NIU) policy and procedures regarding the verification of student identity for distance education to ensure that the student who registers is the same person who participates in and completes a course or program. U.S. Government policy governing security clearances ensure that NIU follows ongoing, systematic procedures for verifying student identity, and ensuring secure login to information systems.
2. **References.**
 - a. U.S. Federal Higher Education Opportunity Act 2008 (HEOA 2008), Public Law 110-315.
3. **Applicability.** This memorandum is applicable to all faculty, staff and students at all NIU locations.
4. **Responsibilities.** The points of contact for this policy and procedures are the Vice President for Finance and Administration; Director of Educational Technology; the Dean, College of Strategic Intelligence; and the Dean, School of Science & Technology Intelligence.

PROCEDURES

5. **Procedures.**
 - A. Security Clearance
 - (1) Each student is required to undergo an extensive background investigation every 5 years, in order to obtain and maintain the Top Secret clearance required to attend the NIU.
 - (2) Clearances will be issued and maintained by the student's home agency or military service.
 - (3) Each student's security clearance status will be checked and verified by the NIU Security Office, NIU-4A, prior to admission being granted.
 - (4) Students who have their security clearance revoked, or otherwise lose access to national security information will be suspended from all programs and access to campus facilities and information systems will be revoked immediately.

B. Information Technology (IT) - Computer System Accounts

- (1) Each student is required to complete Information Assurance training and attend an IT Orientation session during their first year at NIU.
- (2) Unclassified, Secret, and Top Secret computer system accounts are required for student attendance in most NIU programs. Part-time students registered at Academic Centers or other instructional sites may acquire the required computer system accounts from their home agencies. Full-time students are expected to obtain system accounts through their primary NIU location.
- (3) At IT Orientation, each student will obtain a unique username and password for their computer system accounts. Each student must present valid, government-issued identification to receive a username and password. Each student is prohibited from sharing password information at the risk of loss of security clearance, loss of employment and potential criminal prosecution.
- (4) Public Key Infrastructure (PKI) is used on classified networks to validate a user's identity and provide access to classified information to which the person has been granted access. PKI certificate users agree to not share the private keys or passwords under the risk of prosecution, loss of security clearance, and loss of employment.

C. IT - Learning Management System Accounts

- (1) At IT Orientation, each student will obtain a unique student ID and password(s) for use on NIU's web-based learning management systems (LMS). Each student must present valid, government-issued identification to receive a username and password. Each student is prohibited from sharing student ID and/or password information under the risk of expulsion, loss of security clearance, and loss of employment.
- (2) Training on LMS use is provided to each student during orientation.

D. Privacy Policy

- (1) Identity verification for students will be completed in person or by secure video-teleconference technologies.
- (2) No sensitive personal information will be recorded from the identification; only the type of identification presented will be recorded along with the student's name.

E. Identity Verification Procedures

- (1) Identity verification for students attending class at the main NIU campus, Academic Center, or instructional site is accomplished using a badge issued by the local government agency or facility, Department of Defense (DoD) Common Access Card (CAC), or by following visitor procedures at the particular agency or facility.
- (2) Identity verification for students attending classes other than at NIU Headquarters may be accomplished using one of the following proxy methods:

- a. Proctors from the NIU faculty or staff check the student's identification in person and verify the work was accomplished by the identified student.
- b. Proctors from the NIU faculty or staff may use Secure Video Teleconference or similar audiovisual technologies to check the student's government-issued identification and watch students take examinations.

[[SIGNED]]
David R. Ellison, Ph.D.
Rear Admiral, USN (Ret)
President