NOCTI Data Sharing Policy

Safeguarding the confidentiality of individual personal information is the responsibility of all organizations and individuals who collect, maintain, access, transfer, or use education or training records. Under the Family Educational Rights and Privacy Act (FERPA), 34 CFR § 99.31(a)(I)(i), NOCTI is provided access to students' personally identifiable information (PII) to deliver agreed-upon assessment services to its student testing customers. NOCTI takes privacy seriously and makes every effort to protect disclosure of PII for all customers.

NOCTI has rigorous security systems and processes in place for the specific purpose of protecting all assessment-related data (ARD). ARD includes PII related to assessment login procedures, scoring, timing, pre-tests, re-takes, and any accompanying education or training records in the form of disaggregated score results.

This policy establishes the general guidelines NOCTI follows with respect to data sharing. Independent data sharing agreements with collaborative organizations or agencies may be signed to outline specific data handling practices and to ensure adherence to this guiding policy.

Data Sharing
NOCTI will:

1. Establish and use appropriate administrative, technical, and physical safeguards to store and protect ARD from being accessed, used, or disclosed to unauthorized parties.

2. Ensure access to ARD is restricted to authorized staff, officials, and agents of the parties who need it to execute their official duties which require access to the information.

3. Ensure appropriate staff training related to the privacy, security, and confidentiality of ARD and will implement training programs as deemed necessary.

4. Require certifying organizations or agencies, which require access to ARD to perform certification activities, to sign a Data Share Agreement ensuring the protection of ARD and specifying the process for transference of ARD for eligible individuals.

5. Determine the acceptable level of risk of disclosure prior to each planned release of ARD. In each specific case, the data will be evaluated for the risk of disclosure within the context that the data will be used. A safeguard strategy that is the most appropriate for that particular context will be utilized.

6. Statistically aggregate, in non-person-specific form, test responses and other information collected in the certification, credentialing, licensure, and test registration and delivery

process and transfer this information to test sponsors and to independent testing centers. Such aggregated, non-person-specific information may be used for quality control, operations management, educational research, and security to enhance, develop, and/or improve certification, credentialing, licensure, testing services, and testing processes. By administering a test through NOCTI, the customer (e.g., school, agency, organization, or institution) gives consent to this non-person-specific data aggregation and the use and transmission of this aggregated statistical data.

7. Release information requested by a judicial order or legal subpoena. With respect to student ARD, the school of record must make a reasonable effort to notify the parent (or eligible student) in advance of compliance, unless the court or other issuing agency has ordered that the contents of the subpoena not be disclosed, or that the protected education records not be included.

8. Release ARD information to state and local juvenile justice authorities, if state law permits, after receiving written certification that the information will not be disclosed to any other agency, organization, or third party without the parent's permission, except as allowed in state law.

Data Security

ARD is stored in electronic format on systems maintained by NOCTI in a secure data center facility located within the United States of America. The measures that NOCTI employs to protect the privacy and security of the ARD while it is stored in that manner are those associated with industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and layered password protection.

NOCTI servers are hosted by a top-ranked Network Operations Center (NOC) with a Tier 3 Data Center. The NOC has multiple redundant connections to the Internet backbone through several carriers located in different cities. Most importantly, it is designed to remain fully operational in the event of a power outage or failure of a major backbone carrier.

QuadNet™ employs RSA 2048-bit encryption. Assessment administration and related program activities occur within an encrypted web session which discourages unauthorized external access (hacking). QuadNet data is securely protected behind firewalls and Secure Socket Layer (SSL) encryption techniques to prevent hijacking and theft. User-response data has redundant fail-over systems, on-site backup, and off-site backup to guard against disaster, loss, and potential down time. NOCTI's data systems are constantly monitored electronically by technical supervisors to ensure data integrity and no interruptions to service.

Data Destruction

NOCTI complies with retention and disposal schedules consistent with applicable laws and state record retention and disposal schedules.

Unauthorized Release of Data

In the event of unauthorized release of ARD by NOCTI, its subcontractors, or assignees in violation of applicable state or federal laws, notification will be made to the affected party(s) in the most reasonable way possible.