

**PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT**

NOCTI has been engaged by the City School District of Albany to provide services. In this capacity, the company may collect, process, manage, store or analyze student and/or teacher/principal personally identifiable information (PII).

NOCTI will provide the district with *CTE assessment and related services, including administering assessments, issuing score reports, badges, and certificates, and providing assessment related data for instructional purposes.*

NOCTI will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by *requiring certifying organizations or agencies, in accordance with NOCTI's Data Sharing Policy, which require access to assessment related data (e.g., PII) to perform certification activities, to sign a Data Share Agreement with NOCTI assuring the protection of data and specifying the process for transference of data for eligible individuals.* *NOCTI* by entering into an Agreement with the School District acknowledges it has reviewed the relevant District policies on safeguarding PII, including but not limited to, Policy 8635 and Regulation 8635.

PII will be stored *in electronic format on systems maintained by NOCTI in a secure data center facility location within the USA.*

Parents may challenge the accuracy of PII held by *NOCTI* by contacting *Lisa Brauher, Project Coordinator, 800.334.6283, 500 North Bronson, Big Rapids, MI 49307, lisa.brauher@nocti.org.*

The *NOCTI* will take reasonable measures to ensure the confidentiality of PII by implementing the following (*describe the following, as applicable*):

- Password protections
- Administrative procedures
- Encryption while PII is in motion and at rest
- Firewalls
- Other: *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.*

NOCTI's systems employ RSA 2048-bit encryption. Assessment administration and related program activities occur within an encrypted web session which discourages unauthorized external access (hacking). 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.

The contractor's agreement with the district begins on *November 11, 2020* and ends on *June 30, 2021*. Once the contractor has completed its service to the district, records containing student PII will be *maintained and secured to ensure access by the school for historical purposes (e.g., compare program scores from one year to another)*. *If at any time the school wishes to have their data removed from NOCTI's systems, a written request must be submitted.*



Authorized Representative
NOCTI

November 11, 2020
Date