ATTACHMENT # 11

Cyber Responsibilities, Liability and Insurance

A. Vendor Protection of Customer Data

1. The awarded vendor shall, at a minimum, comply with all Delaware Department of Technology and Information (DTI) security standards identified in this Request for Proposals and any resultant contract(s).

B. Definitions

Data Breach

1. In general the term “data breach” means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data for the State of Delaware that results in, or there is a reasonable basis to conclude has resulted in :

    1. 1 The unauthorized acquisition of personally identifiable information (PII); or

    1. 2 Access to PII that is for an unauthorized purpose, or in excess of authorization,

2. Exclusion

    2.1 The term “data breach” does not include any investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

Personally Identifiable Information (PII)

1. Information or data, alone or in combination that identifies or authenticates a particular individual.

    1. 1 Such information or data may include, without limitation, Name, Date of birth, Full address (e.g. house number, city, state, and/or zip code), Phone Number, Passwords, PINs, Federal or state tax information, Biometric data, Unique identification numbers (e.g. driver's license number, social security number, credit or debit account numbers, medical records numbers), Criminal history, Citizenship status, Medical information, Financial Information, Usernames, Answers to security questions or other personal identifiers.

2. Information or data that meets the definition ascribed to the term “Personal Information” under §6809(4) of the Gramm-Leach-Bliley Act or other applicable law of the State of Delaware.

Customer Data

1. All data including all text, sound, software, or image files provided to Vendor by, or on behalf of, Delaware which is occasioned by or arises out of the operations, obligations, and responsibilities set forth in this contract.

Security Incident

1. Any unauthorized access to any Customer Data maintained, stored, or transmitted by Delaware or a third party on behalf of Delaware.

C. Responsibilities of Vendor in the Event of a Data Breach

1. Vendor shall notify State of Delaware, Department of Technology and Information (DTI) and Government Support Services (GSS) without unreasonable delay when the vendor confirms a data breach. Such notification is to include the nature of the breach, the number of records potentially affected, and the specific data potentially affected.

    1. 1 Should the State of Delaware or the awarded vendor determine that a data breach has actually occurred; the awarded vendor will immediately take all reasonable and necessary means to mitigate any injury or damage which may arise out of the data breach and shall implement corrective action as determined appropriate by VENDOR, DTI, and GSS.

    1. 2 Should any corrective action resultant from Section B.1.1. above include restricted, altered, or severed access to electronic data; final approval of the corrective action shall reside with DTI.

    1. 3 In the event of an emergency the awarded vendor may take reasonable corrective action to address the emergency. In such instances the corrective action will not be considered final until approved by DTI.

    1. 4 For any record confirmed to have been breached whether such breach was discovered by the awarded vendor, the State, or any other entity and notwithstanding the definition of personally identifiable information as set forth at 6 *Del. C.* § 12B-101 the awarded vendor shall:

        1.4.1. Notify in a form acceptable to the State, any affected individual as may be required by 6 *Del. C*. § 12B-101 of the Delaware Code.

        1.4.2. Provide a preliminary written report detailing the nature, extent, and root cause of any such data breach no later than two (2) business days following notice of such a breach.

        1.4.3. Meet and confer with representatives of DTI and GSS regarding required remedial action in relation to any such data breach without unreasonable delay.

1.4.4. Bear all costs associated with the investigation, response and recovery from the breach, such as 3-year credit monitoring services, mailing costs, website, and toll free telephone call center services.

D. No Limitation of Liability for Certain Data Breaches

1. Covered Data Loss

   1. 1 The loss of Customer Data that is not (1) Attributable to the instructions, acts or omissions of Delaware or its users or (2) Within the published recovery point objective for the Services

2. Covered Disclosure

   2.1 The disclosure of Customer Data as a result of a successful Security Incident.

3. Notwithstanding any other provision of this contract, there shall be no monetary limitation of vendor's liability for the vendor's breach of its obligations under this contract which proximately causes a (1) Covered Data Loss or (2) Covered Disclosure, where such Covered Data Loss or Covered Disclosure results in any unauthorized public dissemination of PII.

E. Cyber Liability Insurance

1. An awarded vendor unable to meet the DTI Cloud and Offsite Hosting Policy requirement of encrypting PII at rest shall, ***prior to execution of a contract***, present a valid certificate of cyber liability insurance at the levels indicated below. Further, the awarded vendor shall ensure the insurance remains valid for the entire term of the contract, inclusive of any term extension(s).

2. Levels of cyber liability insurance required are based on the number of PII records anticipated to be housed within the solution at any given point in the term of the contract. The level applicable to this contract is: **level 4 (100,001 – 500,000 PII records)**. Should the actual number of PII records exceed the anticipated number, it is the vendor's responsibility to ensure that sufficient coverage is obtained (see table below). In the event that vendor fails to obtain sufficient coverage, vendor shall be liable to cover damages up to the required coverage amount.

Level	**Number of PII records**	**Level of cyber liability insurance required** (occurrence = data breach)
1	1-10,000	$2,000,000 per occurrence
2	10,001 – 50,000	$3,000,000 per occurrence
3	50,001 – 100,000	$4,000,000 per occurrence

4	100,001 – 500,000	$15,000,000 per occurrence
5	500,001 – 1,000,000	$30,000,000 per occurrence
6	1,000,001 – 10,000,000	$100,000,000 per occurrence

F. Compliance

1. The awarded vendor(s) is required to comply with applicable security-related Federal, State, and Local laws.

G. Media Notice

1. No media notice may be issued without the approval of the State.

H. Points of Contact – Data Breach

1. State of Delaware

   Department Of Technology and Information

   Department of Education

Contact information will be provided when signing the contract.