

DATA SECURITY AGREEMENT

This Data Security Agreement (Agreement) is agreed upon effective _____ (Date) by and between _____ County School District and North East Florida Educational Consortium (NEFEC).

1. Disclosure of District Data;

NEFEC shall not disclose District data in any manner that would constitute a violation of state or federal law or the terms of this agreement including, without limitation, by means of outsourcing, sharing, re-transfer, or access, to any person or entity, except:

- a. Employees or agents who actually and legitimately need to access or use District Data in the performance of duties to the District ; and
- b. Any other third party approved by the District in writing and in advance of any disclosure, but only to the extent of such approval.

2. Use of, Storage of, or Access to, District Data

NEFEC shall only store District Data:

- a. In accordance with, and only to the extent permissible under this Agreement and the Contract; and
- b. In full compliance with any and all applicable laws and regulations, only to the extent applicable to Contractor, but without limitation: Family Educational Rights and Privacy Act (FERPA) and, Health Insurance Portability and Accountability Act (HIPAA).

3. Safeguarding District Data

NEFEC agrees that storage and access to District Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. NEFEC shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of District Data. NEFEC shall also implement and maintain any safeguards required to be implemented by applicable state and federal laws and regulations.

Such safeguards shall include as appropriate, and without limitation, the following:

- a. System Security. A System that is owned or operated by NEFEC and contains District Data shall be secured as follows:
 - i. NEFEC shall implement controls reasonably necessary to prevent a breach.
 - ii. The System shall use secure protocols and encryption to safeguard District Data in transit.

- iii. NEFEC shall implement safeguards reasonably necessary to protect its System from compromises and attacks. NEFEC will protect the System with firewalls.
- iv. NEFEC shall:
 - a. Limit administrative access to the System,
 - b. Limit remote access to the System,
 - c. Limit account access and privileges to the least necessary for the proper functioning of the System,
 - d. Remove or disable applications and services that are not necessary for the proper functioning of the System,
 - e. Use named user accounts and not generic or shared accounts,
 - f. Use Federated Single Sign On, Kerberos, or other industry compliant services for authentication and authorization, and
 - g. Enable an appropriate level of auditing and logging for the operating system and applications.
- v. The System shall allow the changing of System and user passwords.

4. Data Protections

- I. NEFEC shall only store District Data:
 - 1. In accordance with, and only to the extent needed to provide services to University; and
 - 2. In full compliance with any and all applicable laws, and regulations
- II. NEFEC shall implement controls reasonably necessary to prevent unauthorized use, disclosure, loss, acquisition of, or access to District Data. This includes, but is not limited to personnel security measures.
- III. All transmissions of District Data by NEFEC shall be performed using a secure transfer method.

5. Definitions

- a. District data: District Data is any and all data that the District has entrusted to NEFEC. For the purposes of this Agreement, District Data does not cease to be District Data solely because it is transferred or transmitted beyond the District's immediate possession, custody, or control.
- b. Data Breach: The unauthorized access and acquisition of computerized data

that materially compromises the security or confidentiality of confidential or sensitive personal information maintained by the District as part of a database of personal information regarding multiple individuals and that causes or the District reasonably believes has caused or will cause loss or injury to any District constituent.

- c. System: An assembly of components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (network, server, computer, software, application, operating system or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- d. Change Management: A formal process used to ensure that changes to a system are introduced in a controlled and coordinated manner. This reduces the possibility that unnecessary changes will be introduced to a system, that faults or vulnerabilities are introduced to the system, or that changes made by other users are undone.

XXXX County School District

North East Florida Educational Consortium

Signature: _____

Signature: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____