COLORADO
Department of Education

ADDENDUM

Overview

The Colorado Department of Education is required by law to collect and store student and educator records, and takes seriously its obligations to secure information systems and protect the privacy of data collected, used, shared and stored by the Department. In the event that Personally Identifiable Information (PII) must be shared with other entities, there is a very strict set of policies and standards that must be followed, and may be found at the following link: http://www.cde.state.co.us/cdereval/approvalprocessdocs

CDE's standards include requirements for protecting CDE data at rest and in transit within an environment at least as secure as protections in place at CDE. Those requirements are summarized in this document below.

In addition to the policies that govern these steps, a formal Data Sharing Agreement must be in place between CDE and any entity receiving CDE data, prior to any data sharing. Data Sharing Agreements and what they contain are explained in more detail at http://www.cde.state.co.us/cdereval/checklistforpiiagreements

This document outlines the minimum data environment that must be in place at an external entity prior to receiving any PII from CDE, for all vendor contracts executed or renewed after the date of this agreement.

Assurances Required to Accept CDE Data

Data Consumers receiving PII from CDE must incorporate the following requirements:

- ✓ Strong access control must be in place. All data must be at a minimum protected with a complex password, workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended. Passwords must be confidential and sharing of passwords is prohibited, must not be written down or stored in an insecure location, and periodically changed and not reused or a reasonable time period.
- ✓ Unused and terminated user accounts must be disabled and/or deleted immediately; account inactivity must be periodically assessed for potential stale accounts.
- ✓ Care must be exercised in inadvertently sharing data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.
- ✓ Systems must be in place for logging and monitoring access and use of data.

- ✓ At a minimum, annual intrusion penetration/vulnerability testing will be implemented.
- ✓ Laptop/mobile device password locks and full disk/storage encryption are required.
- ✓ Data at rest on central computing systems must be encrypted; any backup, backup media, removable media, tape or other copies must also be encrypted, and not used to transport data.
- ✓ Mandatory annual Security awareness training on how to handle PII is required.
- ✓ Appropriate endpoint security anti-virus and anti-malware software must be installed and maintained on computers accessing or processing PII.
- ✓ Transmitting data must occur via a secure method such as Secure File Transfer Protocol (SFTP) or comparable and never sent via email or transported on removable media.
- ✓ Physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.
- ✓ Ability to suppress small N-sizes for aggregated student data reports is required.
- ✓ After prescribed use is concluded, data disposal policies must apply for cleaning up all data. This includes secure scrubbing and securely overwriting data from storage, or physically destroying the storage media.
- ✓ Devices used to copy or scan hard copies of data must have encrypted storage and have storage devices appropriately scrubbed when equipment is retired. Hard copy containing PII is discouraged and must be physically secured, not left unattended, and physically destroyed.
- ✓ All data processing systems, servers, laptops, PCs, and mobile devices must be regularly scanned and have all security patches applied in a timely manner.
- ✓ Data stored in cloud based systems must be protected in the same manner as local data, as described throughout this document. Use of free cloud based services is prohibited, and secondary encryption must be used as appropriate to protect data in cloud storage.
- ✓ Cloud environments, when employed, must be fully documented and open to CDE inspection and verification.
- ✓ Access to cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

Signatures

The entity receiving educational data from CDE (i.e., Data Consumer) agrees to the requirements laid out in this document and the conditions set forth herein.

Signature: _____ *Date:* ___/___/___

[Name]
[Title]
[Organization]