UCPS Data Sharing Agreement Requirements

Protecting the privacy and security of our student data is a challenging, yet critical task. The Department of Public Instruction (DPI) and Public-School Units (PSUs) are required, under Article 29 of NC General Statute 115C, to protect student data. Effective August 1, 2023, all required documentation must be completed before any staff or student information is shared.

This new process is designed to ensure that all NC K-12 school districts have the resources needed to adequately evaluate the security readiness of vendor partners, provide alignment with the State of North Carolina Information Security Manual and the NIST 800-53 framework.

Vendors must meet the following criteria and must be completed prior to the execution of any contract or amendment and revisited annually:

Each vendor and PSU must both sign the DPI (Department of Public Instruction) Data Confidentiality and Security Agreement, in whole with no modifications.

Each vendor must clearly articulate the following items in the Third Party Data Collection Reporting Worksheet:

1. The statewide systems they will be connecting to (PowerSchool SIS, ECATS, Amplify mClass, or any state system containing student information); Including the method of integration (API, AutoComm, SFTP, etc.);
2. Specific data fields requested and the rationale for inclusion within the request, including how the data will be used in the target system;
3. A description of how data will be restricted to the users who have a legitimate business need to see the data;
4. A description of any data written back to the statewide system.

Each vendor must submit the following security documentation:

1. A Vendor Readiness Assessment Report (VRAR) self-assessment to capture the baseline security controls in accordance with NIST 800-53, the framework for state security policies.
2. A third-party conducted assessment report, such as the Federal Risk and Authorization Management Program (FedRAMP) authorization, SOC (Security Operations Center) 2 Type 2 audit, ISO 27001 certification, or HITRUST certification. This report must be no more than 12 months old.
3. Alignment against the NC DIT Statewide Information Security Manual.
4. If a vendor is not in compliance with the Statewide Information Security Manual, additional documentation may be required, including:
    - A third-party conducted penetration test, dated within the last 12 months, with all medium and above findings remediated in accordance with state security requirements.
    - A credentialed vulnerability scan of the environment with all medium and above vulnerabilities remediated in accordance with state security requirements. This scan must be current within the last 30 days and provide a documented report.

All required information may be requested at any time during the contract period.

Submit the Data Confidentiality and Security Agreement, Vendor Readiness Assessment Report (non-State-Hosted -VRAR), AND third-party assessment report to DataSharing@ucps.onmicrosoft.com

For details or additional questions please email DataSharing@ucps.onmicrosoft.com.

Thank you for your partnership with Union County Public Schools