North Carolina Department of
PUBLIC INSTRUCTION

Third Party Vendor Integration Checklist

In order to make sure that the vendor is able to properly and safely integrate into the statewide applications, the PSU and vendor must meet the following requirements based on the security level of the shared data.

Public School Unit:

Vendor Name:

Product:

Does the system share, send or receive data?

□ No (Further action not required)
□ Yes

Phase I: Vendor Selection

□ The vendor, if software as a service, has been told by the PSU they will need to provide the security documents to the PSU initially and on an annual basis.

Phase II: Evaluation

The vendor has provided the PSU the following information about the data they will be collecting in the *Data Sharing Worksheet*:

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

The vendor has provided the the PSU the following security documentation:

□ The NC Vendor Readiness Assessment Report (VRAR) to capture the baseline security controls in accordance with NIST 800-53, the framework for NC state security policies.

□ A third-party conducted assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) authorization, SOC 2 Type 2 audit, ISO 27001 certification, or HITRUST certification to the Department of Public Instruction initially and then annually.

Does the vendor have gaps indicated in their internal controls (from the VRAR)?

□ No

□ Yes, and we have requested the following additional documentation and mitigating controls:

- □ A credentialed vulnerability scan to be provided at execution of the contract and annually thereafter, showing no medium or above vulnerabilities.
- □ A third party penetration test to be provided at execution of the contract and annually thereafter, showing no medium or above findings.

Other:

□

□

□

□

Phase III: Contract Award

□ The PSU has executed the Data Sharing Agreement for Public School Units.

□ The PSU has collected any additional security documentation requested.

□ The PSU has uploaded all information to the DPI Application Portal.

Phase IV: Contract Amendments and Renewals

□ The Vendor has provided any updates on data requirements and the VRAR.

□ The Vendor has provided new security scans (if required), and an updated third-party assessment.

□ The PSU has uploaded all information to the DPI Application Portal.

If the vendor is unable to provide or agree to any of the above the vendor will not be able to the integration cannot proceed.