Linn Benton Lincoln
Education Service District

Code: **DJ-AR**
Reviewed/Revised: 10/20/26

Cybersecurity Review of Purchases and Contracts

1. Scope

A cybersecurity review is required before the ESD enters into, renews or extends any contract, purchase order, agreement, license or subscription with a vendor that will access, store, process, transmit, host or administer ESD data or ESD digital infrastructure. Scope does not depend on dollar value, on whether the purchase is competitively solicited, or on whether the ESD pays for the product or service. Donated, grant funded and pilot products and services are included.

Purchases that involve no ESD data and no access to ESD systems, such as hardware, supplies, furniture and on site labor, are outside this regulation.

2. When the review happens

The requesting department routes the purchase to the Technology and Information Services department before committing to it. Technology and Information Services performs the review and records the outcome. A purchase within scope is not approved to proceed without that record.

A review is required for a new purchase, and again at each renewal or extension. A review already on file may be relied on at renewal if it is current under Section 5.

3. How the review is conducted

The Executive Information and Technology Officer maintains the ESD's vendor security review process, including the risk classification criteria, the security questionnaire, the intake form and the evidence required at each risk level. The process is proportionate: the higher the sensitivity of the data and the broader the vendor's access to ESD systems, the more evidence the vendor must provide.

At the highest risk level, which includes vendors handling confidential data or holding privileged access to ESD systems, the review will include, at a minimum, an independent security audit or certification such as a SOC 2 Type II report or ISO/IEC 27001 certification, confirmation of multi factor authentication and encryption in transit and at rest, and identification of where ESD data is hosted and which third parties can reach it.

Where a vendor will have access to personally identifiable information from student education records, a signed data privacy agreement is required.

A vendor that cannot or will not provide the evidence required at its risk level is treated as higher risk, not lower.

4. Contract requirements

Every contract within scope will require, at a minimum, that the vendor:

- Use ESD data only as necessary to deliver the contracted service, and not for advertising, marketing, resale or the training of models or products.
- Notify the ESD promptly of any security breach affecting ESD data, consistent with ORS 646A.600 to 646A.628.
- Return or securely destroy ESD data at the end of the agreement.

Contracts with vendors at the highest risk level will additionally address encryption, multi factor authentication, subprocessor disclosure and notice, backup and recovery responsibilities, the ESD's right to audit or to receive audit

report summaries, termination for failure to meet security obligations, and Oregon as governing law.

Where a vendor's standard terms cannot be modified, the Executive Information and Technology Officer determines in writing whether the gap is acceptable and what compensating controls apply. That determination is filed with the review record and included in the annual report under Section 5.

5. Insurance

For vendors at the highest risk level, the Executive Financial Officer sets the required insurance coverage based on the vendor's access to ESD data and systems and the size of the contract, and the vendor provides certificates evidencing it. Coverage should address professional liability, network security and privacy liability, and data breach expense. Insurance is not required at lower risk levels unless the Executive Financial Officer determines the contract warrants it.

6. Records and reporting

Technology and Information Services keeps a record of each review, including the risk level assigned, the evidence received, the outcome and the date, and maintains a current inventory of vendors reviewed at the higher risk levels. Records are retained consistent with the ESD's records retention schedule.

A review is current for one year for vendors at the highest risk level and for three years for all others, or until the vendor's service, data handling or ownership materially changes, whichever occurs first.

The Executive Information and Technology Officer reports the vendor inventory, any exceptions granted and any unresolved contract gaps to the Superintendent annually.

7. Exceptions

The Executive Information and Technology Officer may approve a written exception where a requirement is not commercially available from any qualified vendor, or where an emergency purchase is necessary to restore or maintain ESD services. An exception states what is waived, what compensating controls apply and when it expires.

8. Responsibilities

- Requesting department. Identifies purchases within scope and routes them to Technology and Information Services before committing to them.
- Executive Information and Technology Officer. Maintains the review process, conducts or supervises reviews, records outcomes, approves exceptions and reports annually to the Superintendent.
- Data owner, as defined in EHB-AR. Approves how ESD data will be stored, processed and transmitted by the vendor.
- Executive Financial Officer. Sets insurance requirements for higher risk contracts.
- Superintendent. Receives the annual report.

Cross Reference(s):

DJ-AR, Cybersecurity Review of Purchases and Contracts
DJC/DJC-AR, Bidding Requirements
EHB/EHB-AR, Cybersecurity
IIBGA/IIBGA-AR, Electronic Communications System
IGBAB/JO, Education Records/Records of Students with Disabilities
JOB, Personally Identifiable Information