SOLANO COMMUNITY COLLEGE DISTRICT
TECHNOLOGY SERVICES PROCEDURES

THIRD-PARTY RISK MANAGEMENT STANDARD **PROCEDURE # 3910.1**

PURPOSE

This standard is designed to implement a process for Third-Party Risk Management whereby Solano Community College District ("the District") proactively identifies and evaluates the risk profiles of vendors, partners, and suppliers utilized in support of its mission.

SCOPE

This standard applies to any external entity ("the third-party") that is engaged by the District to provide goods, services, or perform functions on the District's behalf. This can include vendors, suppliers, contractors, service providers, consultants, partners, or any other external party that interacts with the District to support its mission.

AUTHORITY

These standards have been authorized and approved by the District's Information Security Officer (ISO) under the ISO's responsibility, as designated by the Board of Trustees ("the Board"), for overseeing, implementing, and enforcing the District's written Information Security Program.

EXCEPTIONS

All exceptions to this standard must be approved by the ISO.

Requests for exceptions to this standard shall be submitted, in writing, to the ISO. The request should specifically state:

- the scope of the exception along with justification for granting the exception;
- the potential impact or risk upon granting the exception;
- risk mitigation measures to be undertaken in conjunction with the exception; and
- a timeframe for achieving the minimum compliance level with the standards set forth herein.

The ISO shall review such requests and confer with the relevant stakeholders. If an exception is granted, it will be documented and reviewed at least annually.

THIRD-PARTY RISK CLASSIFICATION

Prior to contract execution, all third-parties shall be classified as one of two levels of risk: High or Low. To determine the classification of the third-party, the following process shall be completed.

The third-party shall be classified as High risk if the third-party:

- stores, processes, transmits, or interacts with sensitive data in any way; or
- accesses, modifies, or interacts with, any process or technology that could affect the security of sensitive data; or
- maintains any technology located within the District's networks (physical or virtual) that is remotely available over the Internet; or
- is required for District operations such that the District would be negatively impacted if it was unable to perform its role for the District for a time greater than 24 hours; or
- performs or supports a communications role such that it could directly affect the reputation of the District.

THIRD-PARTY CONTRACTS

During the contracting process, third-parties determined to be high risk shall receive greater scrutiny to ensure that they meet the legal, compliance, security, and performance requirements of the District. All high-risk third-party contracts shall include provisions to ensure that the third-party meets the security, compliance, privacy, and performance (e.g., Service Level Agreement) requirements required by the District.

Specific contact language shall be developed in consultation with District legal counsel, but at a minimum, contract provisions should include:

- **Security Measures:** In which the vendor agrees to implement and maintain reasonable and appropriate technical, administrative, and physical security measures to protect the confidentiality, integrity, and availability of District data. (e.g., encryption, MFA, disaster recovery, security awareness, etc.).
- **Documentation Rights:** In which the vendor agrees to, no less than annually, provide documentation to support its compliance with the Security Measures Clause (e.g., third-party assessments, SOC 2, HECVAT, etc.). If a vendor is unable to provide the required documentation, or if documented security controls are deemed to be insufficient, the vendor shall provide a remediation plan to address the concerns.
- **Data Protection and Privacy:** In which the vendor shall handle District data in accordance with all applicable data protection regulations and industry best practices (e.g., FERPA, HIPAA, etc.).
- **Incident Notification:** In which the vendor shall, in the event of a security incident, notify the district promptly, provide detailed information on the incident, implement corrective measures to prevent recurrence of the incident, and bear responsibility for the cost of notification and credit monitoring for affected parties.
- **Data Retention and Destruction:** In which the vendor agrees to retain District data only for the duration necessary to perform the services outlined in the contract. Agreement, and will securely return and/or delete information upon District request or upon termination of the contract.
- **Subcontractor and Third-Parties:** In which the vendor agrees to be responsible for the security of any subcontractors or third-parties.

If pre-existing contracts do not contain the appropriate language, it shall be added no later than upon contract renewal or within 18 months, whichever is sooner.

THIRD-PARTY MONITORING

High-risk third-parties shall agree to provide documentation as to their capability to meet the relevant security, compliance, privacy, and performance requirements of the District no less frequently than annually.

This documentation shall come in one of two forms:

- **SOC 2 Type 2 Report (Preferred)** – System and Organization Controls (SOC) 2 Type 2 is a formal third-party assessment of a third-party's operational controls in protecting information, validating availability of services, and maintaining cybersecurity practices.
- **HECVAT** – Higher Education Community Vendor Assessment Toolkit (HECVAT) is a is a questionnaire framework specifically designed for higher education to measure vendor risk.

Upon receiving this documentation, it shall be reviewed and approved by the ISO, or an appropriately qualified subject matter expert designated by the ISO.

DECOMMISSIONING A THIRD-PARTY

When a third-party's products or services are no longer needed by the District, the ISO shall be notified in writing as soon as possible to begin the appropriate decommissioning processes. These processes should, at a minimum, include the disabling or removing of:

- all access to the District's systems and data;
- all devices within the District's networks (physical or virtual); and
- all system or applications modifications performed to accommodate the third-party (e.g., firewall rules, service accounts, etc.).

CONTACT INFORMATION

All questions or concerns regarding this standard should be directed to the District's ISO.

REFERENCES

- The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule (16 C.F.R. 314.4).
- NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.
- NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations.
- NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.
- NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.
- NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Board Policy 3910

Reviewed by the Governing Board <Date>