SOLANO COMMUNITY COLLEGE DISTRICT

INFORMATION SECURITY POLICY 3910

POLICY

This policy establishes the mandatory minimum information security requirements for the District and defines the responsibility to:

- Protect and maintain the confidentiality, integrity and availability of information and related infrastructure assets.
- Manage the risk of security exposure or compromise.
- Ensure a secure and stable information technology (IT) environment.
- Identify and respond to events involving information asset misuse, loss or unauthorized disclosure.
- Monitor systems for anomalies that might indicate compromise.
- Promote and increase the awareness of information security.

SCOPE

This policy applies to all people, including but not limited to employees, interns, volunteers, contractors, subcontractors, consultants, service providers, and other third-parties, that use or access any IT resource for which the District has administrative responsibility ("users"), including systems managed or hosted by third parties on behalf of the District.

This policy encompasses all systems, automated and manual, for which the District has administrative responsibility, including systems managed or hosted by third parties on behalf of the organization. It addresses all information, regardless of the form or format, which is created or used in support of business activities of the entities.

AUTHORITY

This policy has been authorized and approved by the District's Board of Trustees ("the Board").

The Board formally designates the person serving in the role of Vice President of Technology to be the District's Information Security Officer (ISO). The ISO shall be responsible for overseeing,

implementing, and enforcing the District's written Information Security Program.

Under this authority, the ISO shall periodically, but no less than annually, provide an update on the status of the Information Security Program to the Board.

INFORMATION SECURITY PRINCIPLES

This policy acknowledges that the operation of an institute of higher education is dynamic, and that no Information Security Policy or Program can account for every possible occurrence. Therefore, this policy seeks to establish principles that shall be used to guide all decision-making. These principles shall apply to all subsequent information security policies, programs, procedures, and plans.

- **Defense in Depth –** The District shall follow a principle of Defense in Depth, meaning that the organization shall not rely on the application of any single safeguard to protect the confidentiality, integrity, and availability of the District's systems and data; instead, the District shall layer heterogeneous information security controls to ensure that the organization can prevent, detect, and/or recover from an information security event.
- **Least Privilege –** The District shall follow the Principle of Least Privilege, meaning that access to data and systems shall have only the minimum access feasible to perform the District's objectives. This principle shall apply to all access, whether individual or programmatic.
- **Non-repudiation –** The District shall set a standard of non-repudiation for all users, meaning that no user should have the ability to deny responsibility for performing a specific act on the District's systems or data.
- **Review of Key Controls –** The District shall periodically, but no less than annually, review the efficacy of key information security controls and safeguards identified in the District's Risk Assessment to ensure that they are functioning as designed and intended. This review may include both technical and non-technical testing of controls.
- **Risk Acceptance –** Executive Management, under the advisement of the ISO and based on the District's Risk Assessment and review of safeguards, shall be responsible for establishing the District's risk tolerance, as well as evaluating and accepting risk on behalf of the District.

- **Risk Assessment –** The District shall base the Information Security Program on a written risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, integrity, and availability of District data and systems, and assesses the sufficiency of any safeguards in place to control these risks. The risk assessment shall be reviewed and updated periodically, but no less than annually.

ELEMENTS OF THE INFORMATION SECURITY PROGRAM

The District's Information Security Program shall, at a minimum, include the following elements:

- Acceptable use of technology standards.
- Access control procedures and standards, including Multi-Factor Authentication (MFA).
- Change control procedures and standards.
- Continuity planning, including disaster recovery, business continuity, and cyber incident response.
- Data retention procedures and standards.
- Encryption standards for data in transit and at rest.
- Logging and monitoring procedures and standards.
- Physical and environmental security procedures and standards.
- Secure development practices for custom applications, whether developed by the District or by a third-party on behalf of the District.
- Secure system hardening procedures and standards.
- Security awareness training procedures, including anti-phishing training.
- Vendor and third-party risk management procedures and standards.
- Vulnerability and patch management procedures and standards.

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 Organization
- NIST Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

ADOPTED: June 5, 2024

REVISED:

REVIEWED: