Grossmont-Cuyamaca Community College District Information Security Program

1.0 - Purpose

The Grossmont-Cuyamaca Community College District ("District) is dedicated to maintaining a secure environment for its students and staff. In compliance with laws, policies, and best practices, the District is obliged to protect all personally identifiable information ("PII") digital data in its custody. The Information Security Program ("Program") aims to prevent unauthorized release of PII data and ensure its integrity and availability. This Program outlines the minimum security standards which the District will meet or exceed depending on legal or business requirements and oversees other related security procedures and policies. With this Program in place, the District strives to establish trust with its employees, students, and partners regarding its capability to protect PII data.

2.0 - Scope

This Program includes all PII digital data managed, preserved, sent, or utilized on District systems in line with the District's business operations. It also extends to District workers, volunteers, and vendor partners engaged in tasks directly for the District or its sponsored events.

Moreover, this Program encompasses both physical and virtual systems under the District's management, such as workstations, laptops, mobile devices, servers, network devices, and cloud-based services.

3.0 - Roles and Responsibilities

This Program delineates the subsequent primary roles, current designations, and their related responsibilities:

Role	Current Designation	Responsibilities
Information Security Officer (ISO)	Director of Information Security	An individual appointed by the District who is responsible for the oversight and execution of the Information Security Program, as well as the associated policies and procedures.
Program Reviewer	Associate Vice Chancellor of Technology	A senior member in the District's staff hierarchy who is charged with guiding and supervising the Information Security Officer, capable of granting ultimate approval for the Information Security Program's management when the ISO is not available.

4.0 - Non-compliance

This Program is designed to meet state and federal guidelines for protecting PII data. If there's an event that does not comply with the Program's guidelines, it needs to be reported to the Information Security Officer or the designated Program Reviewer within 30 business days of the incident. Exceptions to the rules of this Program must be clearly detailed, limited in scope, and receive approval from the ISO or the individual authorized to approve the Program exception. Willful non-compliance with this Program that disregards state and federal laws may lead to disciplinary measures, which could include termination of

employment, in addition to legal consequences. All deviations or compliance breaches will be recorded in the current year's annual report on the Information Security Program to the Governing Board.

5.0 - Compliance Requirements

The following are the current state and federal compliance requirements the District with adhere to regarding custody of PII data.

5.1 – Title IV Program Participation Agreement

The District is a participant in Title IV student financial aid programs and concurs with maintaining compliance with the Title IV Program Participation Agreement. Therefore, the District commits to observing the latest requirements of the Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule (16 C.F.R. 314 (2024)). The District also aims to meet the compliance deadlines established by the Federal Trade Commission (FTC) as feasibly as possible, given available resources and operational capacities. Any components that cannot be implemented by the required deadline due to resource limitations, timing, or other business-related factors will be recorded in the annual Information Security Program report submitted to the Governing Board for that year.

The ensuing segments detail the District's baseline adherence requirements for the elements of the GLBA's Safeguards Rule.

5.1.1 - As designated in Section 3.0 - Roles and Responsibilities, the ISO is responsible for overseeing and implementing this Program. Furthermore, a Program Reviewer designated in Section 3.0 will be the senior District member responsible for directing and oversight of the ISO and ultimate approval of the Information Security Program in the ISO's absence.

5.1.2 - The controls for this Program will be guided by an annual risk assessment. This assessment will pinpoint potential internal and external risks to the security, confidentiality, and integrity of PII data that may lead to unauthorized disclosure, misuse, modification, destruction, or compromise. Additionally, it will evaluate the adequacy of existing measures to manage these risks.

5.1.3 – Safeguards tailored to mitigate the risks outlined in annual risk assessments will be assigned a priority and implemented according to the level of risk identified. Additionally, the following security measures will be put into place by the District:

(i) – Periodically review access controls to ensure only authorized individuals can access PII data and that their access is confined to data necessary for their job responsibilities.

(ii) - Evaluate and organize data, staff, equipment, systems, and facilities based on their business significance and within the framework of risk management strategies.

(iii) - Encrypt all PII data under the District's custody during transit and while at rest. If encryption is infeasible, the ISO may approve securing PII data using alternative compensating controls.

(iv) - Follow secure development protocols for internally created applications that handle transmission, access, or storage of PII data, and establish procedures for the security assessment of third-party applications handling such data.

(v) - Enforce multi-factor authentication for every user gaining entry to any of the District's information systems, except when exempted in writing by the ISO for valid business reasons and with compensatory security measures in effect.

(vi) - Aligning with the District's data retention policy, develop methods for the safe disposal of customer information to avoid holding onto PII data unnecessarily. Obligate the erasure of customer data not later than two years after its last use in service provision to the related customer, unless required for ongoing business activities or legal compliance.

(vii) - Implement change management processes for alterations within the production environment.

(viii) - Establish policies, procedures, and mechanisms to monitor and record the actions of authorized users while also detecting any unauthorized attempts at accessing or altering PII data.

5.1.4 - Conduct ongoing testing and monitoring to ensure that access controls for systems and processes remain effective. Penetration tests should occur at least once a year, while vulnerability assessments must be carried out semi-annually to spot potential flaws in the District's cybersecurity measures. Identified critical and high-priority vulnerabilities must be addressed within one year following the penetration test or assessment that detected them.

5.1.5 - Provide security training that is sufficient to address relevant risks or threats identified by the risk assessments, ensure that information security staff keep up-to-date with evolving information security threats and countermeasures, and engage competent service providers to effectively manage information security threats.

5.1.6 - Establish standards for choosing service providers capable of upholding proper protections of PII data, mandate through contractual agreements that these providers adhere to such protections, and annually evaluate the sufficiency of the providers' security measures.

5.1.7 - Review and modify this Program in light of findings from Section 5.1.4, Section 5.1.2, or any other factors that may affect the Program's effectiveness in safeguarding PII data under the District's custody.

5.1.8 - Develop an incident response plan that ensures quick reaction and recovery from any security incidents that could impact the confidentiality, integrity, or availability of PII data under the District's custody.

5.1.9 – Deliver an annual report to the Governing Board of the overall status of the Program, including supplementary items such as any risk assessments, service provider assessments, vulnerability findings, security incident summaries, and updates to the Program.

6.0 – References

This Program references the following standards, policies, and procedures:

- BP 3726 Information Security
- Gramm-Leach-Bliley Act's (GLBA) Safeguards Rule (16 C.F.R. 314 (2024))

- AP 3727 Data Classification
- AP 3728 Email Encryption
- AP 3729 Vendor Risk Management

7.0 – Changelog

Date	Version	Editor	Revision(s)
2024-07-09	2.0	Director, Information Security	Included GLBA Safeguards Rule requirements.