Grossmont-Cuyamaca CCD
Information Systems
Information Security Program

Introduction and Purpose

GCCCD developed this Information Security Program (the "Program") to protect District information and Personally Identifiable Information (PII), as that term is defined below, found on records and in systems owned by the District. This Program is intended as a comprehensive set of guidelines that have been implemented in compliance with regulations issued by the various controlling authorities. This Program will be periodically reviewed and amended as necessary to protect Personally Identifiable Information. This Program should be read in conjunction with other District record-keeping and privacy policies that are referenced at the end of this Program.

The purposes of this document are to:

- Establish a Program for GCCCD with policies designed to secure District information and protect the Personally Identifiable Information of students, alumnae, faculty, and other employees of the District that is maintained by the District;
- Establish employee responsibilities in safeguarding data containing Personally Identifiable Information;
- Outline procedures to implement and administer this Program, including administrative, technical and physical safeguards.

For the purposes of this Program, GCCCD employees include all faculty, staff, contract and temporary workers, and hired consultants and third-party service providers.

Personally Identifiable Information (PII), as used in this Program, means the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Date and place of Birth;
- Mother's maiden name;
- Driver's license number or other state-issued identification card number;
- Passport numbers;
- Medical or biometric information
- Financial account number or credit or debit card number that would permit access to a person's financial account number, with or without any required security code, access code, personal identification number, or password.

Responsibilities

The Information Security Officer (ISO) is in charge of maintaining, updating, and implementing this Program. The ISO reviews incidents of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PII, and, when appropriate, convenes a team of employees to form an incident response task force to determine appropriate responses when a breach occurs. The ISO documents all breaches and subsequent responsive actions taken. Records of breaches are retained by the ISO. All employees and, to the extent relevant, students are responsible for maintaining the privacy and integrity of PII, and are required to access, store and maintain records containing PII in compliance with this Program.

Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual security breaches or unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PII, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the ISO.

Risk Assessment

Risk assessment takes into consideration risks in each relevant area of the District's operations, including employee training, compliance with this Program, and means for detecting and preventing security system failures. The ISO, along with other appropriate employees, has identified and continues to identify the reasonably foreseeable internal and external risks to the security, confidentiality and integrity of information resources and PII that could result in unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of such information. Among the foreseeable risks are external hacks, unauthorized access, thefts, inadvertent destruction of records, unintentional authorization of access, property damage from environmental hazards, and misuse of access by employees, students or business associates.

The ISO and other responsible staff reviews, the sufficiency of safeguards currently in place to control these risks.

Violations

Any employee or student who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises District information or PII without authorization, or who fails to comply with this Program in any other respect, will be subject to the appropriate disciplinary action, which may include termination in the case of employees and expulsion in the case of students. An individual may also be subject criminal charges, depending on the nature of the breech and the intended use of information.

Policies and Procedures for Safeguarding Information

To protect District information and PII, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguards, and training.

Access

- Only those employees, volunteers or authorized third parties requiring access to PII in the regular course of their duties are granted access to PII, including both physical and electronic records.
- Computer access passwords are to be kept confidential and disabled prior to termination of employment.
- Upon termination of employment, physical access to documents or other District information and resources containing PII is immediately prevented.

Storage

- No GCCCD employee may store PII on a laptop or on external devices (e.g., flash drives, mobile devices, external hard drives) without express authorization by the ISO, and such authorization requires encryption of data and other appropriate safeguards.

- Paper records containing PII must be kept in locked files or other secure areas when not in use, and may not be removed from the premises of the District, without the express permission of the ISO.
- Electronic records containing PII must be stored on secure, encrypted servers, and, when stored on authorized desktop computers, must be password protected.

Removing records from campus
- When it is necessary to remove records containing PII off campus, employees must safeguard the information. Under no circumstances are documents, electronic devices, or digital media containing PII to be left unattended in any insecure location.
- When there is a legitimate need to provide records containing PII to a third party, electronic records are password-protected and encrypted, and paper records are marked confidential and securely sealed.

Disposition
- Destruction of paper and electronic records must be carried out in accordance with the GCCCD records procedures, and any other applicable federal, state and local regulations.

Third-party vendor relationships
- The District exercises appropriate diligence in selecting service providers to determine that they are capable of maintaining appropriate safeguards for PII provided by the District to them. The primary budget holder for each department is responsible for determining those third parties providing services to the District that have access to PII
- All relevant contracts with these third parties are reviewed and approved to ensure that the contracts contain the necessary language regarding safeguarding PII. It is the responsibility of the primary cost center managers to confirm that the third parties are required to maintain appropriate security measures to protect PII consistent with this Program and appropriate laws and regulations.

Computer system safeguards
- The ISO monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. To combat external risk and secure the District network and data that contain PII, the District has implemented the following:

Secure user authentication protocols
- Unique strong passwords are required for all user accounts; each employee receives an individual user account.
- Passwords are required to be changed regularly.
- Server accounts are locked after 3 successive failed password attempts.
- User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.

Secure access control measures
- Access to specific files or databases containing PII is limited to those employees who require such access in the normal course of their duties.
- Each employee has been assigned a unique password, different from the employee's password to the computer network, to obtain access to any file or database that contains PII needed by the employee in the course of his or her duties.
- Files containing PII transmitted outside of the GCCCD network are encrypted.
- The ISO performs regular internal network security audits. The ISO reviews computer system logs to the extent reasonably feasible possible electronic security breaches, and

to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of District information or PII.
- All District-owned computers and servers should be firewall protected and regularly monitored.
- Operating system patches and security updates are installed to all servers on a regular basis.
- Antivirus and anti-malware software is installed and kept updated on all servers and workstations. Virus definition updates are installed on a regular basis, and the entire system is tested and checked periodically.

Training

Appropriate initial and periodic ongoing training is provided to all employees who are subject to policies and procedures adopted within this Program or who otherwise have access to PII. The District training department maintains appropriate records of all such training.

Relevant Procedures

The following GCCCD policies and regulations provide advice and guidance that relates to this Program:

- Records Management Policy
- FERPA policy
- Red Flag Policy
- Business Conduct Policy
- Employee Confidentiality Policy
- Responsible Use of Information Technology Resources
- Federal Trade Commission regulations 16 CFR 313.3(n) and 16 CFR 314.1–5; 15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA); U.S. Code 15 USC 6801(b) and 6805(b)(2)
- Gramm-Leach-Bliley Act; sections 501 and 505(b)(2)
- Federal Educational Right to Privacy Act (FERPA)
- U.S. Department of Education regulations on the Integrity of Federal Student Financial Aid Programs under Title IV of the Higher Education Act of 1965, as amended

The District will review this Program at least annually and will change, modify, or otherwise alter this Program as it deems circumstances warrant.