SAN DIEGO MIRAMAR COLLEGE

Guidelines for Protecting Data Sensitivity (GPDS)

Introduction

San Diego Miramar College encourages research on education issues and believes that information should be transparent and available to students, faculty, staff, and the general public. At the same time, the College upholds these guidelines on the access, security, use, and dissemination of sensitive data in order to assure the integrity of research and protect the rights and privacy of personnel and students. The Guidelines for Protecting Data Sensitivity (GPDS) reinforces the exercise of sound judgment and the professionalism of data stewards.

Four principles of data sensitivity were identified including: Data Access, Data Security, Use of Data, and Dissemination of Data. Each principle is discussed relative to three levels of data sensitivity: Level I, Level II, and Level III.

Terms and Definitions

The following terms and definitions are provided in order to establish a shared understanding of the underlying concepts concerning data sensitivity.

Data Sensitivity: The extent to which data should be protected, based on the nature and content of the data

- Level I: Public information which is highly aggregated, or broadly categorized, such as enrollment figures, transfer rates, or any other institution-wide data available at www.sdccd.edu.
- Level II: General request for research reports, survey data, and data that are disaggregated, or broken out by categories, to some extent, such as success rates or student progress at the program level.
- Level III: Special request for research reports and sensitive information that is highly disaggregated, such as student contact information, data at the Course Reference Number (CRN) level, student records, and all personally identifiable information.

Data Specificity: A continuum along which data may be generalized to broad groups or specified to smaller units.

Aggregated Data: Data expressed as total summaries that encompass multiple groups or units within broad categories, i.e., Level I data

Disaggregated Data: Data that are broken out by categories or units (i.e. Level II data or Level III data). If the unit of division is individual students, staff, or faculty members such that the information is personally identifiable.

Data Steward: Any individual who uses, handles, or manages data and is thus responsible for ensuring the security and integrity of the data.

Family Educational Rights Privacy Act (FERPA): A Federal law that prohibits the release of student records (verbally, in writing, or by any other means) without the written consent of the student or a court order or a lawfully issued subpoena, unless there is a specific statutory authorization or a legitimate educational interest or need to know, a need to know as part of fulfilling their job duties, or an emergency (http://www.ed.gov/legislation/FedRegister/finrule/2008- 4/120908a.pdf).

Internet: A world-wide network of computer networks.

Intranet: An internal, private network that can only be accessed within the confines of an enterprise, e.g., the Miramar College "G" drive.

Need-to-know: Necessary for reasonable operation, strategic planning, and the accomplishment of one's expected and stated job duties, while serving a legitimate educational interest.

RRF: Miramar College Research Request Form.

Guidelines for Protecting Data Sensitivity
Statement of Responsibility

I, _____, have read the *Guidelines for Protecting Data Sensitivity (GPDS)*, pages 1 and 2 of this document, in its entirety. I accept the responsibility of protecting the security of data to which I am granted access. I hereby agree to comply with all of the principles, instructions, and regulations related to data access, confidentiality and security, use, and dissemination that are set forth in this document.

_____ _____
[Signature] [Date]

_____ _____
[Signature] [Date]

SAN DIEGO MIRAMAR COLLEGE

Guidelines for Protecting Data Sensitivity (GPDS)

Data Access	Data Security	Use of Data	Data Dissemination
LEVEL I: In order to provide access to all, these data are posted on the San Diego Community College District (SDCCD) web site (research.sdccd.edu). Select data will also be available on the San Diego Miramar College Institutional Research website (http://www.sdmiramar.edu/institution/research). If a requestor of research would like access to Level I data that are not already available, the requestor should complete a Research Request Form (RRF) and follow the RRF protocol delineated in the section below under Level II data. **LEVEL II:** Individuals must complete an Research Request Form (RRF) available at the Miramar College Institutional Research website. RRFs will be processed upon the signed approval by the requestor's supervisors or Department Chairs and School Deans. Supervisors or Department Chairs and School Deans are responsible for ensuring that data are being requested on a legitimate need-to-know basis. Requestors who are new to the process may meet with the Miramar College Research and Planning Analyst. Although the requestor may specify a project timeline, RRFs are prioritized based on the Miramar College College-Wide Research Agenda. External requests, such as those from the press, community, or outside agencies, are to be routed through the Miramar College Office of Planning, Research, & Institutional Effectiveness for appropriate processing.	**LEVEL I, II:** Data reports will be available in PDF format only in order to protect data integrity. **LEVEL II:** All data will be stored on a secure server. Proprietary data will be stored on the Miramar College "G" drive.	**LEVELS I, II, and III:** Data will be: 1) Fairly and lawfully processed. 2) Processed for purposes specified in RFF. 3) Accurate and relevant. 4) Handled with utmost concern for data security. All aspects of research, including formulation of the research question, sample selection, choice of variables, and methodology, should be carefully thought out and planned by Data Stewards (users) with the assistance of the Research and Planning Analyst.	**LEVELS I and II:** The Research and Planning Analyst shall disseminate data as deemed appropriate to requestors who follow the protocol for submitting an RRF. Proprietary data shall be disseminated only with permission. Individuals are obligated to respect all copyright laws and give appropriate credit. Reproductions of data reports should have all original titles, footnotes, and supplemental information intact and unaltered.
LEVEL III: Access will be granted on a need-to-know basis. Individuals who wish to gain access are required to read, print, and sign the GPDS Statement of Responsibility. Individuals who are granted access to Level III data shall be ethically bound to the *GPDS.* In the event that the data requested are not deemed "need-to-know", the data request shall be fulfilled at a more aggregated and appropriate level of data sensitivity.	**LEVEL III:** Access shall be password protected. Passwords will be given to individuals on a need-to-know basis. Data Stewards shall take all precautions necessary to prevent disclosure of highly sensitive data to individuals who have not been granted access. Individuals who have not been granted access shall under no circumstances seek to procure, view, or share sensitive data. Failure to comply with these precautions and restrictions shall meet with serious consequences, as per FERPA. Data Stewards should take care to: 1) Protect the confidentiality of usernames and passwords. 2) Log off or sign out after visiting a password protected Intranet or Internet site. 3) Avoid creating databases or applications that use Social Security Numbers as identifiers. 4) Never send un-encrypted sensitive data via email. 5) Protect printed sensitive data by storing in locked desk, drawer, or cabinet and never leave unattended on desk, copier, FAX, or printer. 6) Dispose of sensitive data by shredding or returning to the Research and Planning Analyst. 7) Physically protect devices that can be easily moved, such as PDAs, laptops, and portable storage devices (e.g., memory sticks).	**LEVEL III:** Highly sensitive data should always be used on a need-to-know basis. These data should never be used for commercial, private, personal, or political purposes.	**LEVEL III:** Highly sensitive data will be disseminated by the Research and Planning Analyst on a need-to-know basis only to requestors who print and sign the *GPDS Statement of Responsibility*. All Level III data that are disseminated by the Research and Planning Analyst will be considered confidential and issues related to confidentiality will be discussed with requestors. Reproductions and unauthorized dissemination of Level III data are prohibited.