San Diego Mesa College
Guidelines for Implementing the Research Planning Agenda (GIRPA)

Introduction

The Guidelines for Implementing the Research Planning Agenda (GIRPA) provide information regarding the proper access, protection, use, and dissemination of data at San Diego Mesa College. 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. The magnitude of data sensitivity is directly related to the scale used for the levels. Moving from one level up to another denotes a significant increase in the data's sensitivity as described in the "Terms and Definitions" section. This document is an evolving work and shall be reviewed and amended periodically.

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
- Level II: General Requests 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 Requests 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
- Aggregate 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

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 Mesa College Intranet

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

Pivot tables: a reporting tool that quickly sorts and summarizes data, independent of the original data layout, in an Excel spreadsheet by dragging and dropping data elements into rows, columns, or summary positions

Guidelines for Implementing the Research Planning Agenda Statement of Responsibility

(*) I, _____, have read the *Guidelines for Implementing the Research Planning Agenda (GIRPA)*, 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: _____

Original: 2/14/07; Revised: 3/14/07; 3/23/074/12/07; 06/18/09; 08/17/09; 02/24/12

San Diego Mesa College
Guidelines for Implementing the Research Planning Agenda (GIRPA)

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 Mesa College Research web site. If a requestor of research would like access to Level I data that are not already available, the requestor should complete a Request for Research Services (RRS) Form and follow the RRS protocol delineated in this document under Level II data. **LEVEL II:** Individuals must complete a RRS Form, available through the Mesa College Research Office or in electronic format on the Research web site. The Research Office will not process RRS Forms until approval is granted from the requestor's Department Chair and School Dean and the Form is received with all required signatures. 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 must meet with the Campus Based Researcher. Although the requestor may specify a project timeline, prioritization of RRSs shall be left to the discretion of the Research Office. External requests, such as those from the press, community, or outside agencies, are to be routed through the Research Office for appropriate processing by the Institutional Review Board (IRB). **LEVEL III:** Access will be granted on a need-to-know basis. Individuals who wish to gain access are required to complete the Data Sensitivity Training Tutorial which will cover proper handling and use of data, comply with the *Guidelines for Implementing the Research Planning Agenda (GIRPA)*, and print and sign the *GIRPA Statement of Responsibility.* Individuals who are granted access to Level III data shall be ethically bound to the *GIRPA.* 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 I:** 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 Mesa College or SDCCD Intranets. Data reports will be available in PDF format only in order to protect data integrity. **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 do not have or have been denied access shall under no circumstances seek to procure or view sensitive data. Failure to comply with these precautions and restrictions shall be met with serious consequences, which range from temporary suspension of access rights to disciplinary action by law enforcement agencies, according to the extent to which security was breached. 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 SSN 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 (shredder available in K202) or returning to Research Office (7) Physically protect devices that can be easily moved, such as PDAs, laptops, and portable storage devices, e.g., memory sticks	**LEVELS I, II, and III:** Data will be: (1) fairly and lawfully processed (2) processed for limited purposes (3) adequate, relevant and not excessive (4) accurate (5) not kept for longer than is necessary (6) processed in line with the Data Subject's right (7) handled with utmost concern for data security (1-7 above adapted from *Data Protection Act 1998 of South Cambridgeshire District, UK).* 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. Data Stewards should ensure data integrity, execute analyses with precision, and interpret findings accurately in a clear, understandable manner. Special attention should be given to data definitions and interpretations of findings. **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.	**LEVELS I and II:** The Campus Based Researcher shall disseminate data as deemed appropriate to requestors who follow the protocol for submitting a Request for Research Services. Data will be disseminated in their appropriate context. Proprietary data shall be disseminated only with permission from the stewards of those data. Individuals are obligated to respect all copyright laws and give credit where credit is due. Reproductions of data reports should have all original titles, footnotes, and supplemental information intact and unaltered. **LEVEL III:** Highly sensitive data will be disseminated by the Research Office on a need-to-know basis only to requestors who print and sign the *GIRPA Statement of Responsibility*. All Level III data that are disseminated by the Research Office will be considered confidential, and issues related to confidentiality will be discussed with requestors. Reproductions and unauthorized dissemination of Level III data are prohibited.