San Diego College of Continuing Education
Guidelines for Protecting Data Sensitivity (GPDS)

Introduction

The Guidelines for Protecting Data Sensitivity (GPDS) provide information regarding the proper access, protection, use, and dissemination of data at San Diego College of Continuing Education. Four principles of data sensitivity are 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, certificates conferred, or any other institution-wide data available at http://www.sdccd.edu.

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; Level III access requires a signature and submission of this document

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 (https://www2.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 San Diego College of ontinuing Education "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: SDCE request for research 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] ______________________________

Original adoption: 2/23/2017

San Diego College of Continuing Education
Guidelines for Protecting Data Sensitivity (GPDS)

Data Access	Data Security	Use of Data	Data Dissemination
ALL LEVELS: **Research Request Protocol:** Individuals must read through the *Guidelines for Protecting Data Sensitivity (GPDS).* Additionally, individuals must complete and submit an electronic *Request for Research Form* to SDCCE's Office of Institutional Effectiveness (OIE) Research and Planning Analyst. Forms are available on San Diego College of Continuing Education (SDCCE) Office of Institutional Effectiveness PRIE website. Request for Research Forms will not be processed until approval is granted from the requestor's Supervisor or Program Chair and School Dean and the Form is received with all required signatures. Supervisors, Program Chairs, and School Deans are responsible for ensuring that data are being requested on a legitimate need-to-know basis. **LEVEL I:** In order to provide access to all, these data are posted on SDCCE PRIE website or on the San Diego Community College District (SDCCD) web site. If a requestor of research would like access to Level I data that are not already available, the requestor should follow the research request protocol above. **LEVEL II:** All requestors should follow the research request protocol above. Additionally, requestors who are new to the process may meet with the Research and Planning Analyst after submission of the Request for Research Form. Although the requestor may specify a project timeline, prioritization of Request for Research Forms shall be left to the discretion of SDCCE's OIE. External requests, such as those from the press, community, or outside agencies, are to be routed through the OIE for appropriate processing. **LEVEL III:** All requestors should follow the research request protocol above. Additionally, access will be granted on a need-to- know basis. Individuals who wish to gain access are required to read, sign, and submit the *GPDS Statement of Responsibility* to the SDCCE's OIE Research and Planning Analyst. 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 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 SDCCE 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 (users) 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 meet with serious consequences 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 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 or returning to 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	**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. **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 SDCE OIE Research and Planning Analyst shall disseminate data as deemed appropriate to requestors who follow the protocol for submitting a Request for Research Form (RRF). Data will be disseminated in their appropriate context. 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:** Highly sensitive data will be disseminated by SDCCE's PRIE Research and Planning Analyst on a need-to-know basis only to requestors who sign and submit 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. Office of Planning, Research, & Institutional Effectiveness San Diego College of Continuing Education