

Introduction

This agreement provides information regarding the proper access, protection, use, and dissemination of data at San Diego City College. 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 levels indicate the magnitude of data sensitivity. To ensure responsible use of data, all individuals who make requests for City College data that are not publicly available are required to complete this agreement at least once every three years. 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: Information which is highly aggregated, or broadly categorized, such as enrollment figures, transfer rates, or any other institution-wide data

Level II: Data that are disaggregated, or broken out by categories, to some extent, such as success rates or student progress at the program level or by student population groups; does not include data disaggregated to the individual level

Level III: Data that are highly disaggregated, such as student-level data, data at the Course Reference Number (CRN) level, student records, and all personally identifiable information

Aggregated Data: Data expressed as 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 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 (<http://www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf>) that prohibits the release of student records (verbally, in writing, or by any other means) without the written consent of the student, except in the case of specific exceptions, which include: a judicial order or lawfully issued subpoena, a legitimate educational interest from a school official, financial aid requirements, , or an emergency

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

Please initial below to indicate you have read this page of the agreement.

[Initial] _____ [Date] _____

Please read and complete the second page of this form.

Data Access	Data Security	Use of Data	Data Dissemination
<p>Individuals who wish to gain access to non-public data are required to read and sign this Data Access Agreement.</p> <p>LEVELS I & II: In order to provide access to all, many reports at these levels are posted on the San Diego Community College District (SDCCD) website at research.sdccd.edu. Select data will also be available on the San Diego City College Research website at sdcity.edu/research. If a requestor of research would like access to Level I or II data that are not already available, the requestor should visit the Research Request web page at sdcity.edu/Research/RequestResearch. Requests from individuals internal to City College who wish to use the data to inform City College operations will be processed upon the approval of the requestor's supervisor/Department Chair and/or School Dean.</p> <p>LEVEL III: Access will be granted on a "need-to-know" basis. Individuals who are granted access to Level III data shall be ethically bound by this agreement. In the event that the data requested are not deemed "need-to-know", the data request may be fulfilled at a more aggregated and appropriate level of data sensitivity.</p>	<p>LEVELS I & II: Data reports will only be available in a non-editable format to protect data integrity.</p> <p>LEVEL III: Access may 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 be permitted to procure, view, or share sensitive data. Failure to comply with these precautions and restrictions shall be met with serious consequences.</p> <p>Data Stewards should take care to:</p> <ol style="list-style-type: none"> (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 sensitive data by storing in locked desk, drawer, or cabinet and never leave unattended (6) Dispose of sensitive data by shredding or returning to the Office of Institutional Research (7) Physically protect devices that can be easily moved, such as cell phones, laptops, and portable storage devices like memory sticks (e.g., by locking in a storage cabinet) 	<p>LEVELS I, II, & III: Data will be:</p> <ol style="list-style-type: none"> (1) fairly and lawfully processed (2) for purposes specified in research requests (3) accurate and relevant (4) handled with utmost concern for data security <p>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 with the assistance of the Office of Institutional Research.</p> <p>Level II or III data should only be used on a need-to-know basis and should never be used for personal purposes without IRB approval.</p>	<p>LEVELS I & II: The Campus-Based Researcher shall disseminate data as deemed appropriate to requestors who follow the protocol for submitting a research request. Individuals are obligated to respect all copyright laws and give appropriate credit, including citations of research reports. Reproductions of data reports should have all original titles, footnotes, and supplemental information intact and unaltered. Research produced in collaboration with City College's Office of Institutional Research is not to be used for publication without approval by the Institutional Review Board.</p> <p>LEVEL III: Highly sensitive data will be disseminated by the Campus-Based Researcher on a need-to-know basis only to requestors who print and sign the <i>Data Access Agreement</i>. All Level III data that are disseminated by the Campus Based Researcher will be considered confidential and issues related to confidentiality will be discussed with requestors. Reproductions and unauthorized dissemination of Level III data are prohibited.</p>

The stipulations outlined in this agreement apply to all requests to the Office of Institutional Research for access to non-public data.

Statement of Responsibility

I, _____, have read the *Data Access Agreement*, pages 1 and 2 of this document, in its entirety. I accept the responsibility for 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.

[Name] _____

[Signature] _____

[Date] _____