

Subject:	Maricopa County Community College District (MCCCD) - Best Practices for Data Security, Acceptable Use and Access Management
Effective Date:	July 1, 2007
Revised Date:	

### Access, Use and Protection of Data

Maricopa County Community College District (MCCCD) recognizes its affirmative and continuing need to protect confidential employee and student data and to maintain the confidentiality of that data.

The MCCCD Data Access and Appropriate Use Best Practice establishes appropriate and reasonable administrative, technical and physical safeguards designed to:

- ensure the security and protection of confidential information in its custody, whether in electronic, paper, or other forms;
- protect against any anticipated threats or hazards to the security or integrity of such confidential information; and
- protect against unauthorized access to or use of such confidential information.
- define standards for obtaining access to data
- define limitations of access and appropriate use of data

[Data](#) are institutional assets used to support instruction, student services and administrative functions. While access and use of data is essential to accomplishing the MCCCD's institutional mission, it requires the observance of critical standards to safeguard individuals' rights that are protected by state and federal laws or MCCCD regulations. Therefore, MCCCD has established a policy consistent with applicable laws regarding access, use and protection of data. The Chancellor shall establish through Administrative Regulation operational standards and practices regarding access, use and protection of data.

#### Authorized Access

MCCCD's intent is to make data as easily accessible as possible for the faculty, staff and administration to accomplish tasks related to their role and responsibilities. Access includes, but is not limited to, varied types of medium such as paper records, printed reports, computer screens, computer systems, electronic storage, and network transmission. Please refer to [Custodian of Record Accountability](#) and [Management and Protection of Data](#) for more information.

#### Acceptable Use

All employees and agents of MCCCD and anyone working on behalf of MCCCD are

charged with the appropriate use of data. Use of data for personal gain without public benefit, or for personal business, or to commit fraud is prohibited. All individuals defined in the scope of this policy are prohibited from negligent or deliberate acts that could result in unauthorized disclosure of data. Please refer to [Principles of Acceptable Use](#) for more information.

#### Reasonable Protection



## Office of the CIO

## Documents of Interest

All employees and agents of MCCCDC and anyone working on behalf of MCCCDC are charged with the protection of MCCCDC data.

Under existing federal and state legislation institutions of higher education are responsible for the confidentiality and integrity of data within their institution. These laws and regulations include but are not limited to:

- The Family Educational Rights and Privacy Act (FERPA) - protection of student records
- Gramm- Leach-Bliley Act (GLBA) - protection of financial records,
- Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002
- The Health Insurance Portability and Accountability Act - (HIPAA) -protection of health care records
- A.R.S. 15-141. Educational Records; Injunction; Special Action

Please refer to [Reasonable Protection](#) for more information.