

Subject:	Management and Protection of Data
Effective Date:	7/1/07
Revised Date:	

Summary:

Purpose

This section of the Maricopa *Data Access and Appropriate Use Best Practice* explains and defines the standards, behaviors, and recommendations for management and protection of Confidential Data aimed at minimizing the potential risks of data compromise which may exist as a consequence of sharing Confidential Data between and among Maricopa entities, or as a result of routine client/server interaction. The Management and Protection of Data define and describe the following:

- objectives for securely storing and disseminating "confidential data".
- objectives and standards for applications using the "primary authentication credentials".
- objectives for the applications accessing the data or directories replicated from the data.

Scope

All employees and agents of Maricopa, anyone working on behalf of Maricopa, and any persons with authorized access to confidential data. This best practice applies to all forms and circumstances of access, sharing, use, manipulation, replication, and retention of Confidential Data within and between Maricopa business units and/or colleges or individuals.

Definitions

Data Steward - Data Stewards are those persons authorized by a college president or vice chancellor or through a process of formal request and approval from a Custodian of record to access, manage, manipulate and disseminate confidential data. Data Stewards differ from Custodians of Record in the following ways:

- They are responsible to Custodians of Record for the approval to gain access to data unless they are delegating previously approved responsibilities of stewardship to an eligible person
- They have no responsibilities for the data regarding response to subpoenas or other legal inquiries
- The justification for access to data generally centers around the development or creation of a system, process or application

Delegate - The formal process of transferring all or a portion of the responsibilities of

stewardship to another person. Recognition that delegation occurred requires that the intent to transfer such responsibilities to another person be made in writing specifying the date of the transfer and the specific responsibilities inherited by the delegate. It also requires a written acknowledgement by the delegate of those specific responsibilities he or she is accepting as of a specific date.

Service Provider - Service Provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to confidential information through its provision of service on behalf of Maricopa or any of its subdivisions.

PRINCIPLES OF MANAGEMENT AND PROTECTION, STEWARDSHIP, AND RESPONSIBILITY

Limitations and Responsibilities

Data Stewards

By reason of organizational role, or through the request and subsequent granting of permission by custodian of record, data stewards are charged with the careful and responsible management of confidential data entrusted to their care. It is the responsibility of the data steward to be informed and knowledgeable of practices and standards related to data or information resource security. As it may be required by his or her job responsibilities, the stewards of confidential data should be able to demonstrate that he or she has taken steps beyond basic actions to mitigate the potential for data compromise or loss resulting from the malicious activity of others.

Delegation of Responsibility

The data steward may delegate any or all responsibilities related to being a data steward to anyone he or she may have a functionally dependent or supervisory relationship with related to managing, developing systems for, or reporting against, confidential data. The delegate of the data steward should have the operational capacity to carry out the duties and responsibilities of stewardship that have been granted to them. The delegate should also be made aware of this administrative regulation, and comply with any procedure regarding the formal acknowledgement of their responsibilities to appropriately use and safeguard Confidential Data. Persons to whom delegation of responsibility has been granted have the same duty as the data steward to adhere to the requirements of this regulation.

Data Stewards With Partial or Limited Technical Infrastructure Responsibility

As a function or limitation of his or her job responsibility, a data steward may not possess responsibility for assessing or correcting vulnerabilities in the information technology infrastructure at the campus or site where an application or system under their care may reside. In such a case, the data steward should make an effort to inform the person or

persons responsible for the security of that infrastructure or vice chancellor of any serious vulnerability that may affect the security of the applications, processes or data under his or her care. Upon receipt of such notification, the person or persons responsible for the information technology infrastructure should take appropriate action to assess the accuracy of such a report, and take any appropriate corrective action.

Responsibilities of Data Stewardship and Use

Approved data stewards should ensure that confidential data entrusted to their care are appropriately safeguarded based upon the following security objectives. Adherence to these objectives also includes the introduction and periodic orientation of applicable staff to the requirements of this best practice.

These security objectives apply, as appropriate, to all users, developers, and administrators or anyone who has access to confidential data including Custodians of Record.