

<b>Subject:</b>	<b>Reasonable Protection</b>
<b>Effective Date:</b>	7/1/07
<b>Revised Date:</b>	

**Summary:**

**Storing Data** - Confidential data should be stored or made available in such a way that access is restricted and authorization required prior to presenting such data to authorized persons or processes. Authorization should be verified at least once at the beginning of each access session and may include but is not limited to the use of access credentials such as a secure username and password, biometric reading, or other forms of user identification/credentials such as cryptographic keys. Steps beyond basic actions may include but are not limited to the use of firewalls, restricted or private networks, physical access security or other techniques or systems designed to stop or mitigate the success of unauthorized attempts to obtain data.

**Access Credentials** - Access Credentials should be used to uniquely identify a process or person, and should not be made public. Access credentials not belonging to or representative of a person are also considered confidential data. Passwords or similar credential components should not be viewable while being entered, or at any time after entry. System passwords or the answers to challenge questions should be saved immediately in a secure repository in encrypted form based upon industry standards.

**Prohibited Credentials -**

- Complete Social Security Number or National ID.
- complete birth date
- a value equal to the username or sign-on credential

**Transport of Data** - Confidential Data during either physical or electronic transport should not be viewable or otherwise accessible to anyone other than the intended recipient. Steps beyond basic actions may include but are not limited to the use of network transport encryption techniques or any system, protocol, or process that is aligned with industry standards, which has the intent of mitigating or limiting the usability of such data in the event it was intercepted while in transport.

**Gathering Displaying Data** - Confidential data while being gathered or displayed should leave no residue such as in web browser caches or any other electronic or manual input device. Data gathering techniques should include steps to mitigate the affects of user impersonation, or other electronic data entry exploits intended to obtain data through errant or malicious entries of instructions, commands, or queries in an electronic input form. Steps beyond basic actions may include but are not limited to the inclusion of field edits, logical result validation, or any other techniques and or software intended to

limit the effectiveness or potential of common data input exploits.

**Disposal of Electronic Data Systems** - Disposal of electronic data systems or storage devices that may have contained confidential data should be accomplished in such a way as to mitigate the possibility that Confidential Data previously stored on such devices could be retrieved or otherwise obtain by unauthorized persons.

**Administrative Data Users** - Maricopa employees who have functional responsibility to develop applications, reports or technical systems that use confidential data are responsible to safeguard such data while it is in their care or possession. Care or possession includes access to and or control of physical documents, or any other form of information generated as a logical or direct consequence of interfacing with administrative systems, and reports, including any data extracted from administrative systems regardless of medium, wherein confidential data is included. As applicable, users should adhere to the standards of data security described above.

**Due Diligence of Service Providers** - The adequacy of the service provider's system of safeguarding information should be determined prior to Maricopa or any of its subdivisions entering into a contractual relationship with the service provider. Maricopa or any of its subdivisions should not contractually engage a service provider who cannot demonstrate that they have a system to safeguard the confidential information that they manage, receive or transfer on behalf of Maricopa. Depending on the service provider, Maricopa may wish to review the service provider's audits, summaries of its test results for security, or other internal and external evaluations. Maricopa or any of its subdivisions should not enter into contractual agreement with any provider who is not capable of maintaining appropriate safeguards for confidential information.

**Service Provider Agreements** - All contracts with service providers should include a privacy clause which requires the service provider to implement appropriate measures to safeguard confidential information and to refrain from sharing any such information with any other party.

Contracts should, when appropriate, include the requirement that in addition to the Maricopa insurance requirements for service agreements, the service provider indemnify Maricopa from financial loss or expense resulting from any requirement to notify victims of security breaches and or any related cost for credit monitoring, or general communication related to the breach of such data.