State of Arizona Accounting Manual

INTRODUCTION

The State of Arizona has in its possession a substantial amount of confidential and sensitive data that it needs to conduct its business. While some State officers and employees need access to certain data, most do not need access to most of this information to do their jobs.

Changes in technology have introduced many efficiencies, such as the ability to transmit documents electronically. However, when electronic documents--such as word processing files, spreadsheet files, forms, or files in a portable document format--are attached as support for transactions in automated systems, such as, but not limited to, AFIS, many individuals without proper need or authority may be able to view or otherwise have access to them. Some of these electronic documents contain confidential or sensitive information--such as, but not limited to, social security account numbers—that should not be disclosed to or shared with all those who might have the ability to view them.

This section of SAAM establishes policies for the electronic transmission and storage of confidential and sensitive information.

POLICY & PROCEDURES

1. When an electronic copy of any file or record is attached in support of a transaction in an automated system, care must be taken by the initiator of the transaction, that, if such file contains confidential and/or sensitive information, those who might have access to such transaction or file must have an operational need and system security to view such information.

1.1. For those statewide automated systems currently in use, systems of user types and data masking accommodate the requirement of protecting confidential and/or sensitive data.

1.2. Agencies should analyze any agency-specific applications it may have (such as licensing systems), to make sure that confidential and/or sensitive information can only be viewed by those with the need and authority to do so.

2. Confidential and sensitive information includes, but is not limited to, the following:

2.1. Social Security Account Numbers (SSNs) and Taxpayer Identification Numbers (TINs).

2.2. Banking information (particularly account numbers and passwords).

2.3. The home addresses of law enforcement and other personnel whose home addresses have been deemed confidential by statute (agency addresses, work addresses and the major cross-streets of an individual's home, however, are not confidential or sensitive).

2.4. Medical information to be treated as confidential under the Health Insurance Portability and Accountability Act (HIPAA).

2.5. Information related to ongoing investigations conducted by the State.

2.6. Information related to ongoing litigation involving the State.

2.7. An individual's rate of pay.

2.8. Levies and garnishments assessed against an employee of the State.

2.9. Any payment card cardholder data required to be controlled by the Payment Card Industry Security Standards Council (PCI). (Additional information concerning PCI can be found in various SAAM sections contained in SAAM Topic 40, *Revenues and Receipts*).

2.10. Any information that is confidential or confidential as so designated by any Federal, State or local law, rule or policy.

3. If, for whatever reason, confidential or sensitive information cannot be obscured when the file is to be attached to a given transaction in an automated system, other means of transmitting the information may be used. This can include transmission by encrypted email, interoffice mail sealed and marked as confidential, or hand delivery.

4. Those in possession of confidential or sensitive information, including the data discussed above, must always exercise care in its storage and, if required, destruction.

4.1. Physical documents containing confidential or sensitive information must be stored in a secured location or device when not in use. These documents should not be left unattended on desks or work stations, where they may be read by those without the need and authority to access such information.

4.2. Electronic documents containing confidential or sensitive information must be stored in an application or file system in such a way that only those with the need an authority can access them.

4.3. Documents containing confidential or sensitive information must be destroyed, not merely disposed of, when no longer needed.

5. Confidential and sensitive information does not include such information as:

5.1. Employee names.

5.2. Employee addresses (other than those discussed above).

5.3. Employee cell or home telephone numbers.

5.4. State-issued Employee Identification Numbers (EINs).

6. Care must be taken, as well, not to leave documents with confidential and/or sensitive material left unattended on printers, copiers or facsimile machines.

7. When confidential and/or sensitive information is to be transmitted by email, either as content or by attachment, it must be transmitted using whatever encryption method is available to the email system. If no such encryption method is available, then the confidential and/or sensitive information must be communicated by other means.