

# Data Storage and Transmission Policy

---

*Security*

**STATE ACCOUNTING OFFICE**  
**Security**  
**Data Storage & Transmission Policy**

**EFFECTIVE DATE:** *January 1, 2014*

**REVISION DATE:** *October 6, 2013*

**REFERENCES:** *GTA Policy: Data and Asset Categorization (PS-08-012)*  
*FIPS 199 Standards for Security Categorization*  
*GTA Policy: Data Categorization-Impact Level (SS-08-014)*  
*GTA Policy: Classification of Personal Information (SS-08-002)*  
*GTA Policy: Statewide Data Sharing (PM-07-003)*  
*NIST Special Publication 800-88: Guidelines for Media Sanitization*  
*Georgia Open Records Act (O.C.G.A. § 50-14-1, ET SEQ)*  
*SAO Policy: Data Classification Policy*

---

[Purpose](#)

[Scope](#)

[Roles and Responsibilities](#)

[Data Storage and Transmission Policy](#)

[Exceptions](#)

[Compliance](#)

[Glossary and Definitions](#)

[Appendix A – Preparing files for Transmission via eMail](#)

**PURPOSE**

The State Accounting Office's (SAO) goal is to create such an environment where increasing the sharing of data between agencies will benefit the State of Georgia (SOG) and its constituents by supporting business process improvement, reducing redundancy, securing electronic data in transmission and allowing more responsive service to data requesters. Adhering to this Data Storage & Transmission Policy assists in improving SAO system data security as well as securing the applicable SOG agency or organization data (as defined in the SAO Policy: [Data Classification Policy](#)) that is transferred or transmitted between SAO managed systems and non-SAO managed systems in accordance with Georgia Technology Authority (GTA) policies and applicable State and Federal laws.

**SCOPE**

This policy pertains to the storage and transmission of confidential data (obtained by employees in the course of performing job duties) for all SAO system data, and SOG agency or organization data maintained within SAO managed systems, regardless of the environment where the data resides. SAO managed systems include: TeamWorks (PeopleSoft Financials and Human Capital Management), Concur, Hyperion and supporting servers. This policy specifically covers data that has been classified as confidential data is defined within the SAO Policy: Data Classification Policy.

The term data includes:

- Electronic information both internal and external to SAO
- Visual or paper information that is shared and/or filed internal to SAO

All employees and third parties who request data from SAO should be made aware of and adhere to this policy. The Roles and Responsibilities section below describes this process flow.

**ROLES AND RESPONSIBILITIES**

**Note:**

*For further definition of the roles and responsibilities see the SAO: Data Classification Policy.*

The requesting party may be either:

- Within the State: SAO/State Agencies
- Third Party: External vendors, companies, contractors, and individuals.

If confidential data is to be shared / transmitted with third parties, they will be bound by Data Sharing Agreement to abide by SAO's Data Storage & Transmission Policy. The party requesting data to be transmitted from SAO shall complete the Data Sharing Agreement found [here](#).

Regardless of the party requesting the data, the Data Owner will need to approve the means of transmission on the Data Sharing Agreement.

Once the Data Sharing Agreement is submitted to SAO, the requesting party will be contacted by SAO so the appropriate discussions and approvals can be gathered and the transmissions can be setup.

Role	Definition
<b>Data Owner</b>	Data owners must approve the means of transmission on the Data Sharing Agreement. If the Data Owner is initiating the request, then the Data owner shall submit and approve the Data Sharing Agreement.
<b>Data Steward</b>	The Data Steward reviews the Data Sharing Agreement and if approved, coordinates with SAO ISO to begin data sharing. They further will respond to any objections from the ISO and work with the Data Owner to determine whether any alternatives are available.

Role	Definition
<b>SAO Information Security Officer (ISO)</b>	The ISO will review Data Sharing Agreements with Data Steward prior to any data transfer. The ISO will verify the transmission method requested (e.g. Secure file transfer, Connect:Direct, etc.) is appropriate for the classification of the data.
<b>Third Party</b>	The Third Party shall submit the Data Sharing Agreement when requesting data to be transmitted from SAO. The Data Owner will need to approve the means of transmission. Once the data has been transmitted, the Third Party will take over responsibility for protecting the data upon receipt.

---

## DATA STORAGE AND TRANSMISSION POLICY

Confidential data should be protected with administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. Confidential data is prohibited on portable devices and non-state owned devices unless prior written approval from the Data Owner (or delegated authority) has been granted.

The classification levels are defined in the SAO Policy: [Data Classification Policy](#). SAO data associated with each Data Classification may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the process being assessed.

The minimum requirements on how to protect the privacy and security of confidential data at varying sensitivity levels while at rest and in the transmission process are as follows:

Method	Within State Usage (SAO/State Agencies)	Third Party Usage (External vendors, companies, and individuals)	Cost	Description	Example (not all conclusive)

<p><b>Encrypted File via Email</b></p>	<p><b>X</b></p>	<p><b>X</b></p>	<p>SAO: Server charge  Data Requesting Party: No cost</p>	<p>Use this means of transmission <u>sending an occasional file</u> directly to an individual within and outside the State.  Features:  <ul style="list-style-type: none"> <li>• Cost effective</li> <li>• Convenient</li> <li>• Files are manually encrypted and sent as an attachment within the email. The password can be provided separately by phone, email, or in person.</li> <li>• Requires 7-zip. (See Appendix A for details)</li> </ul> </p>	<ul style="list-style-type: none"> <li>• Vendor Master file</li> <li>• Vacant position extracts</li> <li>• Leave extracts</li> <li>• Personally identifiable information</li> </ul>
<p><b>Encrypted File via Shared Drive</b></p>	<p><b>X</b></p>		<p>SAO: Server charge  Data Requesting Party: No cost</p>	<p>Use this means of transmission <u>sending directly to an individual</u>. Use this method only if access is restricted to those with a need to know by permissions settings or passwords.  Features:  <ul style="list-style-type: none"> <li>• Cost effective</li> <li>• Convenient</li> <li>• An email can be sent with a link to the file stored on the “shared drive. The password can be provided separately by phone, email, or in person.</li> <li>• Requires 7-zip. (See Appendix A for details)</li> </ul> </p>	<ul style="list-style-type: none"> <li>• Vendor Master file</li> <li>• Vacant position extracts</li> <li>• Leave extracts</li> <li>• Personally identifiable information</li> </ul>

SFTP	X	X Must include Pretty Good Privacy (PGP) encryption	SAO: Server charge Data Requesting Party: No cost	<p>Use this means of transmission when <u>routinely sending files outside and within the State</u> when there is a concern for the confidentiality, availability, and integrity of the files being sent. Good for automated jobs.</p> <p>Features:</p> <ul style="list-style-type: none"> <li>• Encrypts the username/password.</li> <li>• Encrypts data being transferred.</li> <li>• Requires generating and exchanging keys with recipients.</li> <li>• SFTP is more secure and tends to be more reliable than FTP.</li> </ul>	<ul style="list-style-type: none"> <li>• KK - Budget Journal Upload</li> <li>• AP - Prompt Pay sampling</li> <li>• Purchase Card - Federal Bill</li> <li>• Personnel extracts</li> <li>• Personally identifiable information</li> </ul>
------	---	--	--	---	---

<p><b>Accellion</b></p>	<p><b>X</b></p>	<p><b>X</b></p>	<p>SAO: Subscription fee  Data Requesting Party: No Cost</p>	<p>Used this means of transmission when needing to send secure files directly to an individual or team for secure file collaboration.</p> <p>Features:</p> <ul style="list-style-type: none"> <li>• All files on an Accellion system are encrypted in transit and at rest.</li> <li>• Data in transit is encrypted with Triple Data Encryption Standard (TDES) (168 bits) or Advanced Encryption Standard (AES) (128/256 bits) depending on the web browser.</li> <li>• Accellion uses AES encryption for data at rest.</li> <li>• Web interface file upload/download</li> <li>• Track and monitor senders and recipients of all files for data leak prevention.</li> <li>• Monitor content of files shared for data leak prevention.</li> <li>• Federal Information Processing Standard (FIPS) 140-2 Certified module</li> </ul>	<ul style="list-style-type: none"> <li>• Department of Audits and Accounts (DOAA) requests</li> <li>• Network diagrams</li> <li>• Personally identifiable information</li> </ul>
-------------------------	-----------------	-----------------	--	---	--

<b>Connect: Direct</b>	<b>X</b>	<b>X</b>	SAO: Approximately \$6,000/yr.  Data Requesting Party: Approximately \$6,000/yr.	Connect:Direct is a point to point secure file transfer. Connect Direct is SAO's preferred transmission means for <u>use when batch integration is needed to routinely send files</u> with banking or credit card info due to the security and additional features of the tool over SFTP.  Features: <ul style="list-style-type: none"> <li>• Encrypts data being transferred.</li> <li>• Connect:Direct is a faster solution than other valid means of transmission previously defined.</li> <li>• Assures delivery via automated scheduling, checkpoint restart, and automatic recovery/retry.</li> <li>• All activity and statistics are logged with verifiable audit trails of all actions.</li> <li>• Ensures customer information stays private through a proprietary Protocol.</li> </ul>	<ul style="list-style-type: none"> <li>• Electronic Fund Transfers (EFT's)</li> <li>• Positive Pay file</li> <li>• Bank Recon file</li> <li>• Personally identifiable information</li> </ul>
----------------------------	----------	----------	--	--	--

Additionally, data classified as confidential has requirements on labeling / marking as defined in the table below, which specifies the minimum requirements of privacy and security protection for confidential data at varying sensitivity levels while in storage or during transmission.

<b>Scenario for the Data</b>	<b>Confidential: Sensitive Data / *Personally Identifiable Information (PII) Records</b>	<b>Recommended Protection Methods</b>
<b>Access</b>	Confidential data should be protected from view by unauthorized individuals; both while in use and when unattended, as well as, stored in	<ul style="list-style-type: none"> <li>• Background Checks</li> <li>• Confidentiality</li> </ul>

	<p>locked desks, cabinets, or offices within a physically secured building.</p> <p>Access should be granted to individuals with explicit job related need to know basis only.</p>	<p>Agreements</p> <ul style="list-style-type: none"> <li>• Physical Security</li> <li>• Access Control Lists</li> <li>• Monitor Privacy Screens (For individuals who work with confidential data such as payroll information)</li> </ul>
<b>Marking</b>	<p>Confidential data is to be clearly marked as "Confidential".</p>	<ul style="list-style-type: none"> <li>• System output will be marked at footer with word "Confidential"</li> </ul>
<b>Physical Transfer (reports or paper documents)</b>	<p>Paper documents must be transferred in a sealed container / envelope.</p>	<ul style="list-style-type: none"> <li>• Data should only be printed when there is a legitimate need</li> <li>• Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement</li> <li>• Data should not be left unattended on a printer/fax</li> <li>• Copies must be labeled "Confidential"</li> <li>• Must be sent via Confidential envelope; data must be marked "Confidential"</li> </ul>
<b>Electronic transfer (e-mail, FTP, etc.)</b>	<p>Transmission should be granted to individuals the Data Owner has determined there is a business essential need to share. The requesting party must complete a Data Sharing Agreement if requesting transmission of data from SAO.</p> <p>Document based information (e.g. Word or</p>	<p>Use: approved transmission means defined within this policy and further defined by data requested in the Data Sharing Agreement.</p>

	<p>Excel documents) should be password protected or encrypted if transferred via an external network.</p> <p>Only approved encrypted electronic email or encrypted electronic file transmission may be used. See <b>Appendix A</b> for details on preparing files for transmission via email.</p> <p>If confidential data needs to be transmitted over the Internet, it must be sent using encryption.</p>	
<b>Data Storage</b>	<p>Physically control access to system media (paper and digital) and protect confidential data using encryption technologies and/or other substantial mitigating controls. Storage is prohibited on portable devices and publicly accessible systems unless prior written approval from agency or organization head (or delegated authority) has been granted. Approved storage on portable devices or publicly accessible systems must be encrypted.</p>	<p>Use:</p> <ul style="list-style-type: none"> <li>• Full Disk Encryption (Laptops)</li> <li>• Lock laptops</li> <li>• Password protect accounts, files, etc.</li> </ul>

The following means of transmission are not acceptable means of transmission for confidential data and should not be used **at any time** when transmitting confidential data:

Method	Typical File Type	Direction
Personal Email	Any	Inbound / Outbound
Cloud file-sharing sites (i.e. box, dropbox, google drive)	Any	Inbound / Outbound
Personal unencrypted Universal Serial Bus (USB) drives	Any	Inbound / Outbound
Instant Messaging (i.e. Brosix, AOL Instant Messenger, Googletalk, Yahoo Messenger, etc)	Any	Inbound / Outbound

Data classified as public is unrestricted as to its means of storage at rest or transmission and public data may utilize any of the above means of transmission.

## **EXCEPTIONS**

Exceptions to this policy must be approved by SAO Information Security Officer (ISO) with review by the SAO Chief Information Officer (CIO). In each case the request for exception, the agency or vendor must include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the management approval. Denials of requests for exceptions may be appealed to the State Accounting Officer.

## **COMPLIANCE**

Violation of this policy may result in disciplinary action, which may include termination for employees and temporary staff, or a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of SAO information system access privileges, and to civil and criminal prosecution.

## GLOSSARY AND DEFINITIONS

**Advanced Encryption Standard (AES)** - is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

**Clear** - One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method.

**Confidentiality Agreement (CA)** – is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes, but wish to restrict access to or by third parties. It's a contract through which the parties agree not to disclose information covered by the agreement.

**Data at Rest** – all data in storage but excludes any data that frequently traverses the network or that which resides in temporary memory. Data at rest includes but is not limited to archived data, data which is not accessed or changed frequently, files stored on hard drives, USB thumb drives, files stored on backup tape and disks, and also files stored off-site or on a storage area network (SAN).

**Degaussing** - is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.

**Disintegration, Pulverization, Melting, and Incineration.** These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

**Federal Information Processing Standards (FIPS)** - are publicly announced standardizations developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract.

**File Transfer Protocol (FTP)** - is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

**National Institute of Standards and Technology (NIST)** – known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory, also known as a National

Metrological Institute (NMI), which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

**Personally Identifiable Information (PII)** - is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

**Pretty Good Privacy (PGP)** - is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

**Purge** - Degaussing and executing the firmware Secure Erase command are acceptable methods for purging.

**Secure Shell (SSH) File Transfer Protocol** - is a network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream. It was designed by the Internet Engineering Task Force (IETF) as an extension of the Secure Shell protocol (SSH) version 2.0 to provide secure file transfer capability, but is also intended to be usable with other protocols. Also known as Secure File Transfer Protocol, or SFTP.

**Shredding** - Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.

**Triple Data Encryption Standard (TDES)** - is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

**Universal Serial Bus (USB)** - is an industry standard developed in the mid-1990s that defines the cables, connectors and communications protocols used in a bus for connection, communication, and power supply between computers and electronic devices.

## APPENDIX A PREPARING FILES FOR TRANSMISSION VIA EMAIL

All email transmission of confidential data from SAO must utilize an encryption mechanism between the sending and receiving entity. Guidelines for preparing files for email transmission are as follows:

**Emailing Confidential Data:** Do not include confidential data in the body of an email. Encrypt all documents containing confidential data. Email the confidential data within an encrypted attachment with the password provided separately (e.g., by phone, another email, or in person).

**Confidential Data on Shared Network Drive:** Store encrypted confidential data on shared network drives (“shared drives”) only if access is restricted to those with a need to know by permissions settings or passwords. Email the link where the confidential data is stored within the shared drive with the password for the file provided separately (e.g., by phone, another email, or in person).

**NOTE:** In SEPARATE methods (i.e. by email, phone or in person), send the password to recipients. This should be done before or after sending the link and/or the encrypted confidential file. NEVER send in the same email.

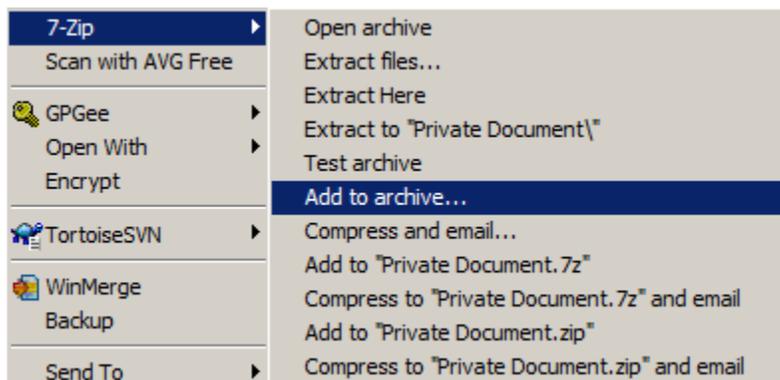
### PROCEDURES FOR ENCRYPTING FILES

SAO uses and recommends 7-zip file archiver for encrypting files that will be sent via email. Directions for encrypting files are as follows:

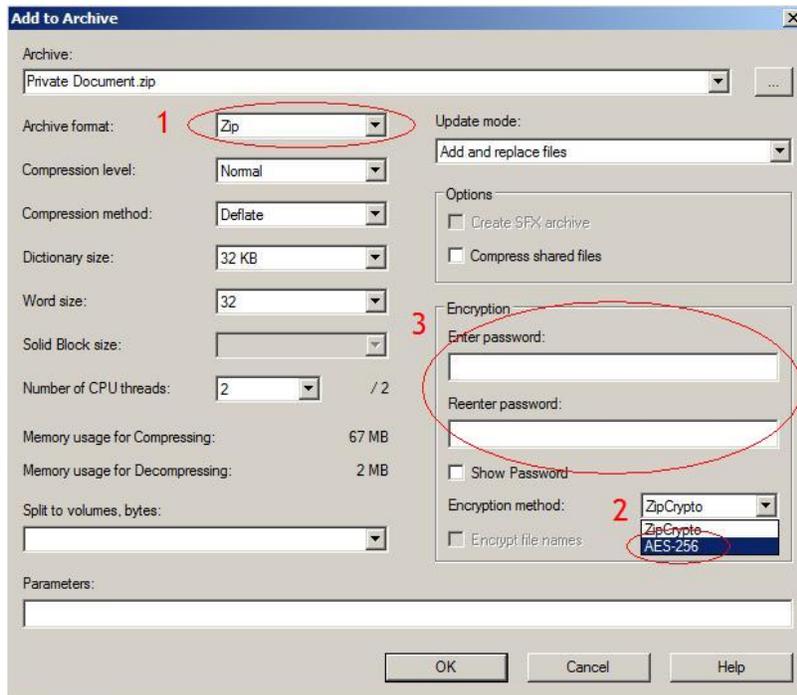
#### A. Encrypting a File with 7-zip

As default 7-Zip installs itself to with “explorer extensions” that allow you to right click on items on the desktop or in windows explorer to compress files. Z-Zip has its own file format 7z which is more efficient at compressing files than the standard zip extension, but this will mean the person you are sending the file to will also have to use 7zip. Using the zip format will enable people using other programs to decompress the file.

1. Right click on the files or folder you wish to compress and encrypt.



2. Change the Archive format to Zip (or use 7z if both you and your intended recipient use 7zip)



3. Change the encryption method to the robust AES-256, thirdly enter your password. Then click OK. The rest of the options can be left as default.
4. You have successfully created the new Zip file which has the file encrypted and password protected in it. The new Zip file can now be attached to an email or stored on a shared network drive.

### Decryption

5. Simply right-click on the file, select extract then enter the password when requested.

DRAFT



200 Piedmont Ave  
Atlanta GA 30334  
[sao.georgia.gov](http://sao.georgia.gov)