



STATE ACCOUNTING OFFICE Confidentiality Policy

EFFECTIVE DATE: July 24, 2014

PURPOSE

Many employees work with information, processes, or data that must be kept confidential in order to protect the interests of the agency, our customers, and our employees.

STANDARD

Information regarding applicants, customers, or employees shall not be divulged to anyone other than persons who have a legitimate need to know. Division Management are responsible for identifying confidential information used in their Division and for assuring proper handling of confidential records. When in doubt as to whether certain information is or is not confidential, no disclosure shall be provided without first obtaining management authorization. This policy extends to both external and internal disclosures.

To protect confidentiality, employees are reminded to:

- A. Store confidential information in locked files or secure area when not in use;
- B. Avoid displaying confidential data where it can be easily observed;
- C. Avoid discussing confidential information except when required to perform the job; and
- D. Immediately inform their supervisor of any loss of confidential information.
- E. Place all discarded confidential information in the shredding bins located on each floor.
- F. Removing confidential information from the agency premises is prohibited unless previously approved by Division Management for work purposes.

Inappropriate use, disposal or disclosure of confidential information can result in civil or criminal penalties, both for the individuals involved and the Agency. Confidential information obtained as a result of employment with the Agency is not to be used by an employee for the purpose of furthering any private interest, or as a means of making personal gains. Employees who violate this policy may be subject to discipline up to and including termination.



STATE ACCOUNTING OFFICE Confidentiality Policy

Projects administered by the agency may stipulate additional confidentiality guidelines and requirements. Respective project managers will be responsible for informing their employees of these additional guidelines.

Additional confidentiality guidelines include but are not limited to:

- Infringement of any copyright, trademark, patent or other intellectual property rights.
- Performing any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of system/network performance.
- Unauthorized distribution of state data and information.
- Use of another employee's access for any reason unless explicitly authorized.

State Accounting Office personnel provide essential and valuable services to agencies, vendors, and state employees. While engaging in these functions, employees collect or may have access to utilize personal and privileged information concerning individuals associated with State of Georgia agencies, vendors, and employees.

This requires a commitment of confidentiality to protect privacy. To ensure the privacy and security of data review the lists below:

TO DO

- Access, distribute, share, and retain confidential data only as authorized and only as needed to conduct agency business as required to perform my job duties.
- Store under secure conditions all confidential data that I retain and ensure its confidential and timely destruction when no longer needed to conduct agency business as required by my job.
- Respect the confidentiality and privacy of individuals whose data I access.
- Observe any ethical restrictions that apply to data to which I have access.
- Protect confidential information located at my workstation.
- Report immediately to my supervisor any and all apparent and suspected security breaches.
- Comply with agency security policies and procedures.

NOT to DO:

- Discuss verbally or distribute in electronic or printed formats any confidential data except as authorized and as needed to conduct agency business as required to perform my job duties.
- Make unauthorized copies of confidential data.
- Knowingly falsely identify myself.



STATE ACCOUNTING OFFICE Confidentiality Policy

- Gain or attempt to gain unauthorized access to confidential data or state or agency computing systems.
- Share my user ID(s) and password(s) with anyone nor use anyone else's user ID(s) or password(s), except as authorized.
- Leave my workstation unattended and unsecured while logged-in to state or agency computing systems.
- Use or allow other persons to use state/ agency data for personal gain.
- Engage in any activity that could compromise the security or confidentiality of data held in State Accounting Office records.

All agencies, vendors and employees have a right to privacy and all employees and contractors are expected to treat all sources and records as privileged. Consultation with a higher level supervisor is required if there is any doubt or question about the authority to release information.

Please note that violations of this policy subjects employees and contractors to disciplinary action, up to and including termination.