

## WHAT STAFF SHOULD DO DURING DATA CLEANUP

During the Data Cleanup campaign all employees are encouraged to locate and then securely delete or archive any sensitive data files found on their computer. If time permits, sensitive documents should also be located and depending on the retention requirement for the document it should be securely destroyed, or archived.

To determine how long a sensitive and non-sensitive business related document or file must be retained by the Institute, employees can reference the Board of Regents (BOR) data retention guidelines, which are located on the Resources page of the data cleanup website.

It is important that every employee is aware of the sensitivity level and value of the Institute data that may be stored on their computer and in the office. Employees can determine the classification of their data, by reading and becoming familiar with the Georgia Tech Data Security Classification Guide. The guide is designed to be used as a reference tool and to provide tips and other general information regarding specific data types. A complete copy of the guide can be found on the Resources page of the Data Clean Up website [www.datacleanup.gatech.edu](http://www.datacleanup.gatech.edu).

Employees are encouraged to work closely with their CSR to locate the sensitive files on their computer, and with their manager to determine if the files should remain on their computer or be securely deleted or archived to the department's fileserver if one is available.

Sensitive files containing social security, credit card, and gtID numbers can be located on the computer by running a discovery tool name Cornell Spider. The tool was created by Cornell University, but modified by Georgia Tech to work more efficiently in our environment. Your CSR can either install the tool by visiting your computer or by using a centrally managed console such as LanDesk.

Once the tool has been installed and ran on the computer, the employee should do the following:

1. Review the report and follow the path of the file listed in the report to locate each file identified as containing sensitive data.

**Note:** Employees may have to work with their CSR to assist with following the path to locate the sensitive files.

- a. Once located the employee will have to determine if they need to securely delete, archive, or keep the files on their computer.
  - i. The files should be securely deleted if not needed for the employee's current job duties
  - ii. The files should be archived to the department's fileserver if one is available and the files are needed to perform the current job duties
  - iii. The files should be archived to removable media such as a CD/DVD, encrypted USB drive etc. and stored in a securely controlled location such as a locked desk drawer, a safe, or file cabinet, if a fileserver is not available however and the files must be retained for the current job function.

**Note:** The files should only remain on the computer if they can not be secured on the fileserver or secured removable media, or if the Department Head approves keeping the sensitive data on the computer. Systems that must continue storing sensitive data should be encrypted using the GT approved PGP whole-disk encryption application. A license for the application will be issue by OIT to all computers approved by the Dean to continue storing sensitive data.

- b. As the employee is locating and reviewing their sensitive files, they should also be updating the Spider report to indicate how they handled each file (i.e. securely delete, archive, or keep).

The Spider report should be pulled into an application such as Microsoft Excel by the CSR or employee, so that additional information can be added to the report by the employee to indicate whether or not they securely deleted, archived, or need to keep the sensitive file.

- c. Once the employee has viewed each file and updated the report, the report should be reviewed by the employee's manager for approval of the distribution (i.e. *securely delete, archive, or keep*) of each sensitive file.

### **Important Notes:**

1. The CSR or faculty member may choose to verify that sensitive files that are not needed have been removed from the computer by running Spider again and comparing the reports.
2. The spider log file contains information to the location of files that contain sensitive data. It is important that the CSR move the file off the system as soon as possible.

FOR MORE INFORMATION REGARDING DATA CLEANUP, VISIT [www.datacleanup.gatech.edu](http://www.datacleanup.gatech.edu)  
FOR SUPPORT OR QUESTIONS, E-MAIL [datacleanup@gatech.edu](mailto:datacleanup@gatech.edu)