

WHAT TO DO DURING DATA CLEANUP IF YOU ARE A CSR/CSS

1. Identify a secure place for employees to archive their sensitive files such as a departmental fileserver.
 - a. If a fileserver does not exist and can not be obtained to secure the sensitive files, the CSR should provide each employee with a manageable and auditable solution to securely store the sensitive files that need to be removed from the desktop (*i.e. removable media such as CD/DVD, Encrypted USB Drives, etc.*)

Note: All removable media must be stored in a securely controlled location such as a locked desk drawer, a safe, or file cabinet.

2. Run the GT configured Spider sensitive data discovery tool on all systems in the department. Spider is an application created by Cornell University to “crawl” a computer and search for social security, credit card, and gtID numbers.

GT has modified Spider to run more efficiently in the GT environment by adding a list of exceptions to decrease the amount of false-positive items in the report. A complete list of the exceptions can be found in the Spider installation guide. The Cornell Spider application and installation guide can be downloaded from the OIT Software Distribution website, under the CSR/CSS Affiliation section.

- a. Install the Spider sensitive data discovery tool on all systems in the department
 - i. Spider can be installed on multiple systems by using LanDesk to push the application to multiple systems.
 - ii. Spider can also be installed as a stand-a-lone application by visiting each system.
- b. Once Spider is finished running, a report will be generated and the results will be written to **C:\spider.log**
- c. The CSR should then pull the results into Microsoft Excel or another tool that can view text files, so that the system owner can follow the file path and view each of the files tagged as containing sensitive information.

Note: Depending on the skills of the system owner, the CSR may have to assist them with following the path to locate the sensitive files.

- d. The system owner will also need to have a way to edit the report to note whether they are deleting, archiving to a fileserver, a removable media such as CD/DVD, encrypted USB drive; or if they need to keep the file for job performance.
- e. Once the system owner has viewed each file and updated the report, the report should be reviewed by the system owner’s manager or department head for approval of the distribution (*i.e. securely delete, archive, or keep*) of each sensitive file.

Note: For information on the employee, manager and department head responsibilities, please read the coordinating section on this data cleanup site.

3. Upon approval from the manager and/or the department head regarding the distribution of the sensitive files, the CSR will be responsible for appropriately securing and maintaining the fileserver containing the sensitive files that were removed from the desktop and archived to the server.
 - a. If a fileserver does not exist, and sensitive files were archived to removable media, the data owner/employee or CSR must store the media in a securely controlled location such as a locked desk drawer, a safe, or file cabinet.

Note: Spider is also available for Macintosh OS X, Linux and Unix operating systems and can be downloaded from Cornell University’s website at <http://www.cit.cornell.edu/security/tools/>

Important Notes:

1. The CSR may be asked by the manager or department head to verify that sensitive files that are not needed by the employee have been removed from the employee’s 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
FOR SUPPORT OR QUESTIONS, E-MAIL datacleanup@gatech.edu