

WHAT TO DO DURING DATA CLEANUP IF YOU ARE A DEPARTMENT HEAD

As part of the President's commitment to reducing Tech's risk of sensitive data exposure by decreasing the amount of sensitive data stored on employee's computers and in their office, Department Heads are asked to encourage if not require every employee in the department to do the following to locate sensitive digital files:

1. Have the CSR run the Spider sensitive data discovery tool on their computer(s).
 - a. If the employee's computer is self managed, meaning not managed by an IT professional (i.e. the CSR), then the employee should run the tool on their computer.
 2. The employee should then review the results of the Spider report.
 - a. The report will list all sensitive files containing social security, credit card and gtID numbers found on the computer.
 3. The employee should then take the time to located each sensitive file listed in the report and make a decision to do one of the following:
 - a. Securely delete the files if not needed to perform their job
 - b. Archive the files to the department's fileserver if the sensitive files are needed frequently for job performance.
 - c. Archive the files to a removable media such as a CD/DVD, or encrypted USB drive if the sensitive files are not needed frequently and a department fileserver is not available.
- Note:** All removable media must be stored in a securely controlled location such as a locked desk drawer, a safe, or file cabinet.
- d. Encrypt the hard drive if the files need to be frequently accessed or can not be archived to a fileserver and must remain on the employee's system for job performance.
 - i. OIT will provide a copy of the PGP encryption application for each system that must continue to store sensitive information for job performance.

Note: Encryption should be used as a last result. The goal is to remove sensitive data from the desktop to minimize data exposure.

If appropriate steps are taken by the employee, the CSR, and the department manager, at the end of the campaign the department head should have a list of all systems in the department that continue to store sensitive information.

The Department Head is then responsible for the final sign-off/approval on the list of servers and faculty/staff system(s) that will continue to store sensitive information, therefore requiring encryption. If the department head determines that a system should not continue to store sensitive information, the employee must securely delete or archive the data based on the department head's direction.

The Department Head should then forward the approved form to atacleanup@gatech.edu

The Department Head is also asked to encourage employees to do the following to locate sensitive paper files:

1. Look through file cabinets and other storage locations for paper files such as old PSFs, travel authority forms and any other document that may contain social security or credit card numbers, as well as spreadsheets with student grades.
2. Once the files are located, these documents should be reviewed to determine if they fall within the BOR retention requirement:
 - a. If yes and the documents need to be accessed frequently, the document(s) must be stored in a securely controlled location such as a locked desk drawer, a safe, or file cabinet for the duration of the required BOR timeframe.
 - b. If yes and the documents do not have to be accessed frequently, the document(s) can be archived to the Library's off-campus Archives & Records Management facility for safe storage.

- i. This service should only be used if the files require long-term storage. Files that need to be accessed frequently should not be stored off campus.
- c. If no the documents can be destroyed using the campus secure Recycling service by boxing the materials, taping the box top, and labeling the box sensitive/confidential.
 - i. Recycling will pick up free of charge 10+ boxes from your department or building.
 - ii. Departments or buildings with 1 – 9 boxes can drop them off at the on-campus Recycling department.
- d. If no and a small amount, the documents can be shredded in the department by the employee.

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