

WHAT TO DO DURING DATA CLEANUP IF YOU ARE A MANAGER

1. During the data cleanup campaign the department and/or business managers will be responsible for reviewing the final Spider report of each of their direct reports and determine if the employee has deleted or archived to a fileserver, CD/DVD, or encrypted USB drive.
 - a. Using the department's fileserver is preferred for archiving the sensitive information. If your department does not have a fileserver, then using a CD/DVD, or encrypted USB drive can be used. The media should then be locked in a secured location such as a locking file cabinet or desk drawer.
 - i. The CD/DVD, or encrypted USB drive should be labeled with a destroyed date, so that the media is not left behind for years to come.

Note: A Spider report is generated once the Spider sensitive data discovery tool has been installed and ran on the employee's computer. The CSR should be asked to do this step unless the employee's system 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. All sensitive files that are tagged by the employee as "must keep", the manager should review the files and determine if the employee should keep the files to perform their job function or if the employee should:
 - a. Delete the files if not needed to perform their job
 - b. Archive the files to the department's fileserver, CD/DVD, or encrypted USB drive and stored in a secured location if needed for job performance.
 - c. Keep the files on their computer.

Note: If the files are to remain on the employee's computer, the hard drive is required to be encrypted. This will require approval from the Department Head.

3. If the manager determines that sensitive files should not remain on the employee's computer, the employee must delete or archive the files as instructed by the manager.

Note: If the manager can not determine if the employee should keep a file containing sensitive information, the problem should be brought to the attention of the Department Head.

4. Once the manager has reviewed and signed-off on each of their employee's report, the manager should create a list of all the employees (*if any*) that must keep sensitive information on their computer and provide it to the Department Head so that he or she knows which employees and computers will continue to store sensitive information.
5. If the department head approves the list, the list should be sent to OIT, so that a PGP encryption license can be assigned to each system.
6. If the department head does not approve the list, the manager should work with the specific employee to ensure the sensitive file(s) is/are deleted or archived as instructed by the department head.
 - a. Once the list has been revised as instructed by the department head, the list should be sent to OIT, so that a PGP encryption license can be assigned to each system.

Important Note: The spider log file contains information to which files could potentially contain sensitive data on that system. It is important to move the file off the system as soon as possible. The CSR or manager may also want to verify that sensitive files have been removed from the employee's computer by running Spider again and reviewing the report.

FOR MORE INFORMATION REGARDING DATA CLEANUP, VISIT www.datacleanup.gatech.edu
FOR SUPPORT E-MAIL datacleanup@gatech.edu