UNCG’s Security of Networks and Networked Data Policy (section III.A.iv.f) requires University data classified as restricted¹ to be stored on network file storage facilities that are centrally managed by Information Technology Services (ITS), http://www.uncg.edu/cha/policy_manual/network_security/. The primary purpose of this policy is to minimize the risk of University data being compromised and accessed by unauthorized individuals as a result of a local computer workstation security breach.

ITS has purchased and implemented an enterprise software package, Identity Finder, to assist UNCG faculty and staff in complying with this policy. Once the Identity Finder software is installed on a computer, a report will be generated that will identify all files on the local workstation that potentially contain restricted data. This report is available locally to the user and a copy is stored on a central Identity Finder server for enterprise compliance monitoring as well.

Faculty and staff should use these reports to review files on their workstation(s) that may contain restricted data and take the appropriate action to move the files to network storage space, delete the files², or scrub the files of the restricted data.

ITS will begin a campus wide intensive effort to implement Identity Finder for all faculty and staff and remove restricted data from computer workstation(s) starting this month. There are several ways that UNCG faculty and staff can engage in this process.

1. **Self-Remediation:** Visit the ITS Identity Finder website (http://its.uncg.edu/Identity_Finder/) to obtain a copy of the Identity Finder software and documentation. Run Identity Finder on your computer workstation(s) and remediate any locally stored restricted data.

---

¹ Restricted data are defined as data whose access is controlled by Federal and State laws (e.g. FERPA, HIPAA). Restricted data is not “sensitive data,” such as employee salary data (this information is subject to public records disclosure). Some common examples of restricted data include student records such as grades (FERPA), certain employee records (various NC statutes), and “personal information.”

“Personal information” is defined by the North Carolina Identity Theft Protection Act to mean a person’s first name or first initial and last name in combination with any of the following items:

- Social security or employer taxpayer identification number.
- Driver’s license, State identification card, or passport numbers.
- Checking account numbers.
- Savings account numbers.
- Credit card numbers.
- Debit card numbers.
- Personal Identification Number (PIN code).
- Digital signatures.
- Any other numbers or information that can be used to access a person’s financial resources.
- Biometric data.
- Fingerprints.

Even if listed above, however, “personal information” does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, State, or local government records.

Further information can be found at http://its.uncg.edu/Technology_Procedures/Data_Classification/

² Information that is an official University record, and not a reference or convenience copy of that record, must be managed according to Record Management protocols. See http://its.uncg.edu/Records_Management/ for more information.
2. **Department Technical Staff Remediation:** Contact your department’s technical support staff and request that he/she run Identity Finder on your computer workstation(s) and remediate any locally stored restricted data.

3. **ITS Remediation:** ITS will schedule appointments with faculty and staff (who have not yet remediated their workstation) to run Identity Finder on their computer workstation(s) and remediate any locally stored restricted data.

If your workstation is remediated by ITS, you should expect an appointment at your workstation with an ITS staff member who will assist you in installing the Identity Finder software, running the initial report and moving all files identified by the software as potentially containing restricted data to your network home directory file space. This appointment will take 1 – 1.5 hours to complete and you need to be present for the duration of the appointment.

ITS staff members will not review or make any determination about the files that the Identity Finder software identifies as potentially containing restricted data. These files will only be relocated to your network home directory file space by ITS. It will then be up to you to review these relocated files and determine what course of action you need to take on them to ensure that you remain in compliance with University policy.

More information on Identity Finder can be found on the ITS website at [http://its.uncg.edu/Identity_Finder](http://its.uncg.edu/Identity_Finder). Contact 6-TECH (256-8324) or 6-TECH@uncg.edu if you need further assistance.