Introduction to Identity Finder

This sheet describes the purpose for using Identity Finder and the data classification levels.

1. IdentityFinder is a search tool that allows you to find confidential or sensitive data on computers and promptly remove or secure them. This tool will aid in protecting the data because it is required by FERPA, the Privacy Act, Connecticut records retention regulations, and by College Policy. However, Identity Finder does not work automatically. It will need your manual input to be able to protect or remove the data.

2. IdentityFinder searches for a specific Data Classification Level (DCL) but it can be configured for other levels.

3. DCL0 is given to data that is public information such as advertisements, directory information, press releases, job postings, etc.

What is IdentityFinder?

- Confidential or Sensitive Data
- Requirements: FERPA, Privacy Act, Connecticut records retention regulations, and by College policy.
- Manual Action Required

Data Classification (DCL) Levels

‘Enrollment Blitz’ to include Three Rivers Community College

Published December 28 2015 1:33PM Updated December 28 2015 1:33PM
Introduction to Identity Finder

4. **DCL1** is given to data that is internal such as internal memos, minutes, internal project reports etc. from the community college(s) and the Board of Regents.

5. **DCL2** is given to data that under strictly controlled circumstances can be disclosed. Typically these items are protected by FERPA such as birthdays, mother’s maiden name, academic records, test scores, courses taken, student records, advising records and disciplinary actions, and employee records etc.

6. **DCL3** is protected confidential data. If lost, it can cause identity theft or financial harm to the person. This includes student loan data, bank account information, social security information, and credit card information. Identity Finder by default is set to search for DCL3 data.
7. **Data Domains** are departments in the college that work with DCL3 data. If you work in one of the departments listed in the image, then you have some level of access to DCL3 data and are responsible for protecting that information. Each department has a data steward. If you are not sure of your responsibilities, then ask your department’s data steward.

8. Since Identity Finder can help flag for DCL3 data, a possible solution could be to delete old data. However, it can be difficult to find the data and we are required to follow Connecticut State’s record retention policy. The policy can be found at [www.ctstatelibrary.org](http://www.ctstatelibrary.org).