Spirion Instructions

Office of Information Security

Created by Jeroen Barendse

Updated August 21, 2017

What is Spirion?

Spirion (formerly Identity Finder) is a program that scans for confidential data, also known as Protected Level 1 data.

What is Protected Level 1 Data?

Protected Data is defined by the CSU Data Classification Standard. There are two levels of protected data:

- Level 1, or Confidential, and
- Level 2, or Internal Use

Access, storage and transmissions of Level 1 Confidential information are subject to restrictions as described in CSU Asset Management Standards.

Information may be classified as confidential based on criteria including but not limited to:

a) Disclosure exemptions - Information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws.
b) Severe risk - Information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur.
c) Limited use - Information intended solely for use within the CSU and limited to those with a "business need-to know."
d) Legal Obligations - Information for which disclosure to persons outside of the University is governed by specific standards and controls designed to protect the information.

Examples of Level 1 – Confidential information include but are not limited to:

- Passwords or credentials that grant access to level 1 and level 2 data
- PINs (Personal Identification Numbers)
- Birth date combined with last four digits of SSN and name
- Credit card numbers with cardholder name
- Tax ID with name
- Driver's license number, state identification card, and other forms of national or international identification (such as passports, visas, etc.) in combination with name
- Social Security number and name
- Health insurance information
- Medical records related to an individual
- Psychological Counseling records related to an individual
- Bank account or debit card information in combination with any required

security code, access code, or password that would permit access to an individual's financial account
- Biometric information
- Electronic or digitized signatures
- Private key (digital certificate)
- Law enforcement personnel records
- Criminal background check results

Why do I care about Spirion?

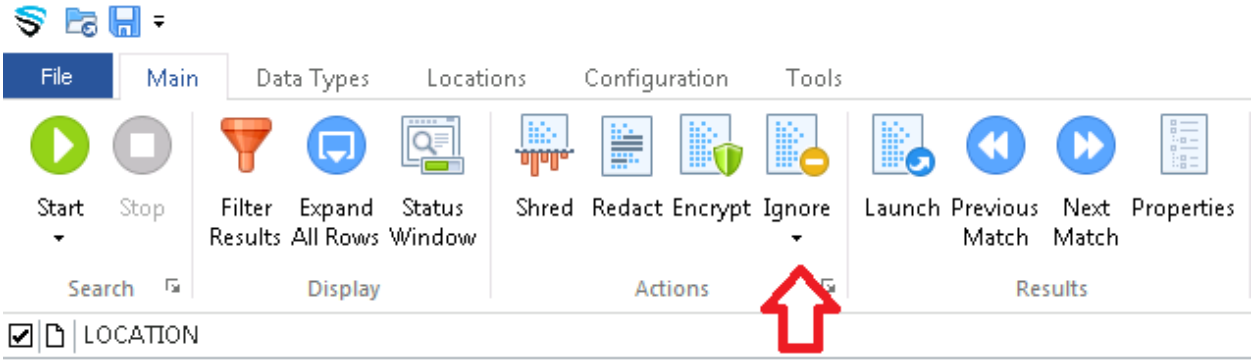
Files containing Protected Level 1 data

The Information Security Office has been scanning each department share on campus using Spirion. Each department is responsible for designating an individual to review the results of the Spirion scan and securing the files flagged as containing protected data.

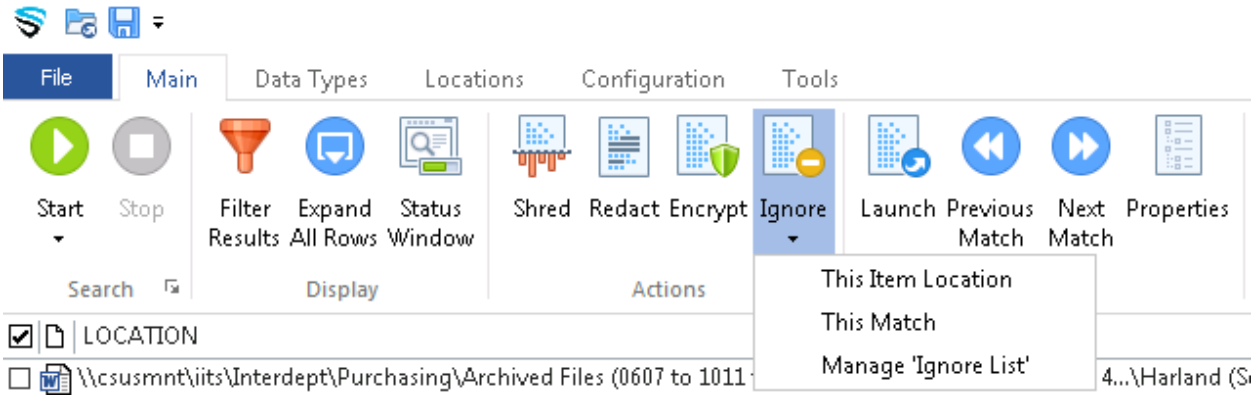
Reviewing the results of the Spirion Scan

Each file flagged by the Spirion scan must be reviewed to determine if it is Protected Level 1 data.

Items that are not protected level 1 data can be ignored using the **ignore** feature in the Main tab of the Spirion ribbon menu:

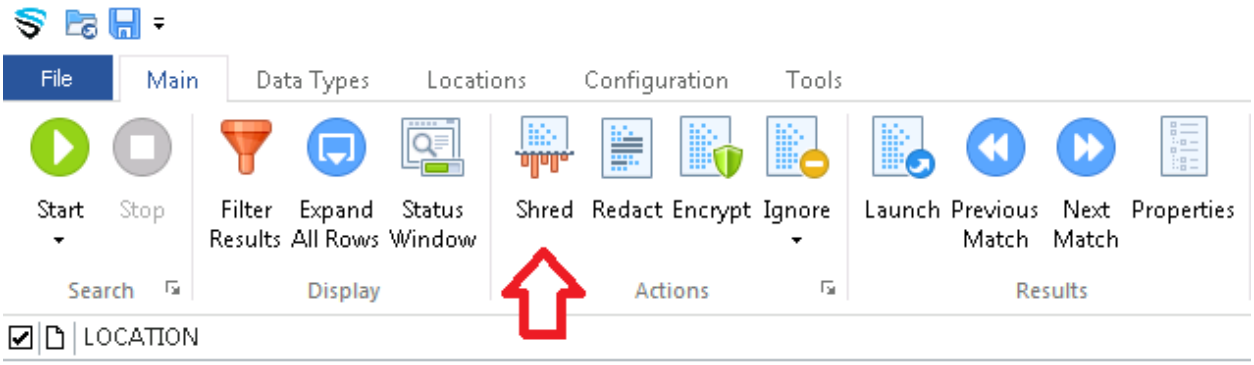


You can ignore either the **identity match** or the **identity location**:

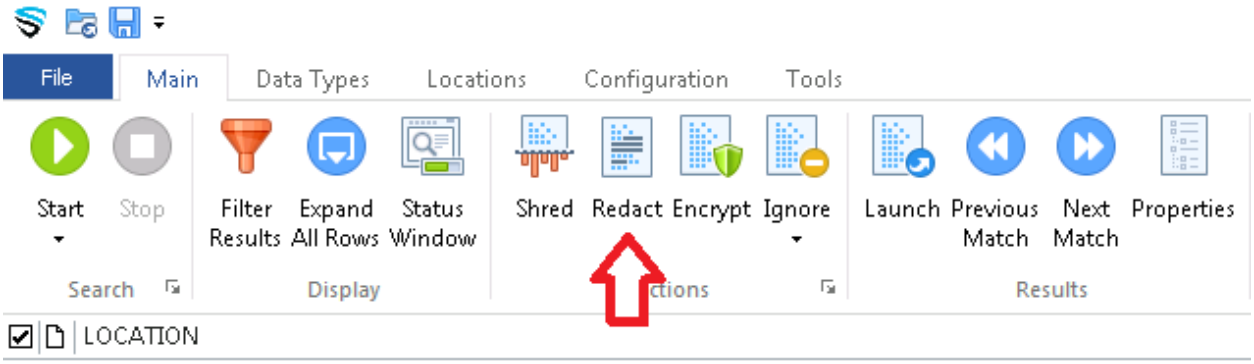


Ignoring the identity match will ignore the flagged item throughout all files. Ignoring the item location will ignore all matches in a flagged file.

Files that have been flagged and are no longer required to be retained due to business processes or State or Federal laws should be deleted using the **shred** feature in the Main tab of the Spirion ribbon menu:



If the flagged file was created in Microsoft Word or Excel, you can remove the protected information from the file using the **redact** feature in the Main tab of the Spirion ribbon menu:



If you are required to retain the flagged protected information, you can encrypt the files using **Azure Information Protection**. Instructions for Azure Information Protection can be found at on the CSUSM Security webpage – Azure Information Protection.*

*Please do not use the Spirion **secure** feature as this method requires a password for encryption. Azure Information Protection allows you to encrypt files using your CSUSM account, and allows you to grant access to other individuals by granting their CSUSM account access.