Security :: Protected Information Scan

The HSU Executive Memorandum on Protected Information [1] requires that Level 1 [2] and Level 2 [3] data not be stored on electronic systems or devices unless absolutely necessary and should be removed when the business reason for storage is no longer required.

The **Protected Information Scan** is used to determine the likely locations of protected data for your further action. It does not determine whether you are authorized to store protected data on your campus computer.

What to do with protected data

If you find protected data on your system, you should do one of the following:

- **Delete it** (if it no longer meets a current business need.)
- **Move it** (to a department file server or a secured removable device)
- **Edit it** (so the document no longer contains sensitive data)

For computers and users with an ongoing need to store protected data that's necessary for conducting essential university business, encryption [4] may be a solution, Encryption should not be used without consultation with your ITC [5].

Note: Identity Finder encryption is NOT recommended.

Working with Protected Information (PI) scanning tools

Depending on the size of your hard drive, the amount of data and the speed of your computer, a PI scan may take a significant amount of time to complete and can limit the impact of other work. **Do not attempt to run a PI scan without first consulting your ITC!**

Click here for an overview of PI scanning tools [6]

Tips for sorting through your results

A positive result does not mean that the type of data found is in fact sensitive. False positives are files that contain pattern matches similar to the form of sensitive data, but which do not actually contain such data. Identity Finder [7] and other PI scanning tools can be used to review potentially sensitive files for accuracy and to eliminate false positives.

Important note

Just because your PI scan did not identify the presence of sensitive information does not guarantee that there is none there. It simply means that the patterns used by the Protected Information scanning tools to search your computer did not find any results.

Related Topics

Data Protection [8], Security [9]

Source URL: http://www.humboldt.edu/its/security-protectedinformationscan

Links:
[1] http://humboldt.edu/policy/PEMP10-03HSU-Implementation-CSU-Data-Classification-Standards
[2] http://www.humboldt.edu/its/glossary/5#term224
[3] http://www.humboldt.edu/its/glossary/5#term293
[4] http://www.humboldt.edu/its/security-encryption
[5] http://www.humboldt.edu/its/glossary/5#term233
[6] http://www.humboldt.edu/its/security-protectedinformationdiscoverytools
[7] http://www.humboldt.edu/its/security-identity-finder-windows
[8] http://www.humboldt.edu/its/category/quicklinks/data-protection
[9] http://www.humboldt.edu/its/category/quicklinks/security