Security :: Protected Information

What is Protected Information?

"Protected information" is an umbrella term for information that is linked to an individual person's identity, such as Social Security numbers, drivers' license data, and credit card or bank account information (sometimes called Personally-Identifiable Information, or PII [1]) and which can be used to facilitate identity theft. Universities in particular have become attractive targets for hackers because of the freedom with which information is exchanged in an educational environment. Humboldt State University, like other institutions, is legally required to be vigilant and proactive in the protection of PII that's been entrusted to us.

The University has issued an executive memorandum [2], the main points of which are described below, which aims to identify and protect private data entrusted to the University. This executive memorandum mandates that all University employees locate existing protected data in their area and either register and protect it or destroy it.

Executive Memorandum

The Executive Memorandum for Protected Information defines data classification standards [3] for Humboldt State University. It also establishes requirements for the protection of Level 1 [4] Protected data and Level 2 [5] Private data stored on campus computers.

- Level 1 and Level 2 data may only be stored on University-owned computers.
- All campus computers must be scanned for the presence of personally-identifiable information (see Protected Information Survey below).

Data Classification Standards

Data classification standards [3] have been developed by CSU to classify various types of information as outlined below:

- Level 1 data: Confidential information governed by existing law or statute such as Social Security numbers and names, credit card numbers with cardholder names, or medical records related to an individual.
- Level 2 data: Internal use information that must be protected due to ethical or privacy concerns such as student grades, courses taken, or disciplinary actions.
- Level 3 data: General information such as a person's title, email address, or other directory information that is available in the public domain.

Detecting Protected Information

The University is required to inventory protected information stored on campus systems. PII detection tools can be used to quickly locate protected information stored on campus computers.

The Protected Information Detection [6] toolkit contains:

- Tools and instructions to assist in locating and scanning for PII
- A form to be completed when campus computers are scanned for PII
- A form to request permission to store Level 1 or Level 2 data if applicable

Handling Protected Data

If you find protected data on a system under your control, the following options are available to you:

- If it no longer meets a business need **- destroy it** [7]
- Paper Shredding Guidelines [8]
- If it needs to be kept - **move it** to a secure and labeled CD or other offline location, or to a secure server, and ensure that it is **encrypted** [9]**.**
- If the protected data is not essential to the document containing that data, **edit it** to remove the sensitive data
- Protected Data: Online Cloud Storage and Email [10]

Remember that HSU protected data may only only be kept on campus systems.

Keeping Protected Data

Level 1 or Level 2 data may only be kept on a system if it meets the following conditions:

- There must be a documented current business need
- Approval has been obtained from the University President or authorized representative using the required form [11].
- The system is using University-supported encryption [9] to protect the data from unauthorized access and is in compliance with HSU-mandated security standards [12].

Related Topics

Data Protection [13], Security [14]

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

Links:
[1] http://www.humboldt.edu/its/glossary/5#term225
[2] https://www.humboldt.edu/policy/PEMP10-03HSU-Implementation-CSU-Data-Classification-Standards
[3] http://www.humboldt.edu/its/security-dataclassificationstandards
[4] http://www.humboldt.edu/its/glossary/5#term224
[5] http://www.humboldt.edu/its/glossary/5#term293
[6] http://www.humboldt.edu/its/security-protectedinformationsurvey
[7] http://www.humboldt.edu/its/security-securedestruction
[8] http://www.humboldt.edu/its/security-paper-shredding
[9] http://www.humboldt.edu/its/security-encryption
[10] http://www.humboldt.edu/its/cloud-storage
[11] http://www.humboldt.edu/its/sites/its/files/docs/PII-authorization-form.pdf
[12] http://www.humboldt.edu/its/security-protectedinformationstandards
[13] http://www.humboldt.edu/its/category/quicklinks/data-protection
[14] http://www.humboldt.edu/its/category/quicklinks/security