3.b Data Security

Responsible Office	Information Technology		
Effective	5/10/2016		
Revised	2/17/2021		
Last Reviewed	2/17/2021		
Compliance	NWCCU 2.C.4, ER 15		
Classification	☒ Institutional	☐ Board of Directors	☐ Local unit(s):
Approving Body	☒ President's Council	☐ Board of Directors	☐ Unit VP

Policy

In support of its educational mission, Heritage University acquires, develops, maintains, and archives information. Some of this information is confidential or restricted, either for the business purposes of the University or for the purpose of protecting the privacy and security of the individuals who work and learn there. This policy is intended to provide guidance and requirements for identifying and protecting the sensitive information with which it is entrusted.

Information with sensitive data is found throughout the campus community in various forms. It is collected, stored, archived and often transmitted by printing, electronically, and orally. Heritage University is committed to protecting the privacy and security of the information entrusted to it. In addition there are legal mandates for securing some of this data. Everyone who handles or has access to sensitive information is responsible for protecting information in a legal, judicious, and secure way.

The guidelines below apply to all confidential data, and where noted to restricted data as well.

1. Limit the collection of confidential data.
2. Limit the use of confidential and restricted data.
3. Minimize the proliferation of confidential and restricted data
4. Secure confidential and restricted data

Compliance with this data protection policy is the responsibility of all members of the University community. Report any privacy incident immediately to your supervisor or Vice President.

Definitions

Personally Identifiable Information (PII): A piece of data or combination of data that permits an entity the ability to uniquely recognize or infer the identity of a person. This data is considered sensitive if, when compromised or disclosed it could result in harm, embarrassment, inconvenience or unfairness to an individual.

Confidential Data - Data which is legally regulated; and data that would provide access to restricted information. All Sensitive PII is considered confidential and must be handled in conformance with the guidelines in this policy.

Restricted Data - Data which while not legally protected could be misused to the detriment of the University, its students, faculty, staff, partners, alumni, donors or other third parties; and data protected by contractual obligations.

Sensitive Data – A term covering both confidential and restricted Data.

Mobile Device – A portable computing device. This includes but may not be limited to laptops, smart phones, tablets, USB flash drives, etc. ALL Heritage-related confidential and restricted information stored on a mobile device *must be encrypted.*

Related Documents

Records Management Policy
Information Technology Appropriate Use Policy
Family Educational Rights and Privacy Act (FERPA) Policy