

Title: Guidelines for Storing and Using Personally Identifiable Information in Non-Production Environments
Effective Date: November 15, 2011
Issuing Authority: Chief Information Security Officer

Policy

Not Applicable

Scope

This guideline applies to all University employees and faculty who in the course of their jobs at Temple University must use confidential or regulatory protected information electronically in non-production systems.

Purpose

Information protected or covered by regulations, such as FERPA, HIPAA, GLBA, PCI-DSS, Pennsylvania Breach of Personal Information Notification Act and other sensitive, private or personal information, must be protected at all times. In order to appropriately protect these information assets; measures must be taken to ensure that the confidentiality, integrity and availability of the data are not compromised. This procedure outlines the steps that employees and faculty should take prior to using or storing sensitive, private, personal or regulatory protected information in non-production (Test) systems.

Definitions

1. Education Records - Any record (in handwriting, print, tapes, film, electronic, or other medium) maintained by the university or an agent of the university that is directly related to a student unless noted under FERPA as an exception.
2. Electronic Media –Technology used to store or transport data in electronic or digital form. Hard, floppy or optical disks, USB drives, memory sticks, magnetic tape, wire, wireless, cable and fiber are among examples of electronic media.
3. Internet – Any portion of a network connection that is not under the direct control and management of Temple University.
4. Non Public Information (NPI) –personally identifiable financial information and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available that should be given special protections to ensure that it is not disclosed to anyone unauthorized under the Gramm-Leach-Bliley Act (GLBA).
5. Protected Health Information (PHI) – the definition given to information that should be given special protections to ensure that it is not disclosed to anyone unauthorized under the Health Insurance Portability and Accountability Act (HIPAA).

6. Regulatory Protected Information – Data which is protected by federal, state or local law and includes, but is not limited to, PHI, NPI, and Educational Records.
7. Sensitive, private or personal Information – Any information that is not for public consumption and if that information were exposed could cause harm to the University or any of its employees, faculty, students, or alumni.
8. Non-Production Systems – systems used for application development, testing, production-support and training. Testing environments include those used for integration, functional, structural (non-functional) testing as well as for user acceptance testing.
9. Test Data – non-production data that does not belong to, or cannot to identify, an individual irrespective of affiliation with the university, and that is used for the purposes of development, integration, functional, structural testing as well as used for user acceptance and training purposes.
10. Production Data – data that belongs to, or can identify an individual, or that is otherwise considered Regulatory Protected Information.

Guidelines

1. As a best practice non-production systems should only contain test data and not copies of production data.
2. The Chief Information Security Officer will permit the use of Production Data in non-production environments on an exception basis. The general criteria for such exceptions are as follows:
 - a. The development or test being completed requires a production level validation with production level data, and
 - b. The non-production system has the same level of security as the production system, and
 - c. The non-production system is on the list of systems that undergo an review by Information Security to ensure data protection standards.
3. If the above conditions are not met, then all sensitive data must be masked or redacted. This requirement covers all fields that contain information that is covered by FERPA, HIPAA, GLBA, PCI, PA Breach Notification Act and any other data deemed that could expose the University or any of its employees, faculty, students, or alumni to harm. See Appendix A for a list of covered date elements.
4. Once it is determined that you need to use production data in a test environment, you must contact the Office of Information Security at 215-204-7077 or at CISO@temple.edu to work out a procedure for having this non-production system reviewed.
5. Use of the Test Data will be allowed for up to *one* year and reviewed annually.
6. Production Data is not to be used in any presentation (live demonstrations or illustrative e.g. Power Point).

7. During training sessions, production data is not to be used unless all users present are authorized to view the data. The training session data and attendees must be reviewed by the Office of Information Security at 215-204-7077 or at CISO@temple.edu.
8. If you are not sure about the sensitivity of your document, please ask your supervisor for guidance. If necessary, contact the Office of Information Security.

Appendix A – Covered Data Elements

1. What needs to be protected?

The following list contains examples of data elements that if used in non-production environments should be masked:

- a. Social security number
- b. National identification number
- c. Driver's license or state issued identification number
- d. Birth date
- e. Birth place
- f. Tax ID number
- g. Bank account information
- h. Credit card account information
- i. Medical records
- j. Certificate/License numbers
- k. Grades
- l. Class lists
- m. Disciplinary records
- n. Student financial records
- o. Payroll records
 - i. For all employees
 - ii. For students worker, assistantships, resident assistants programs
- p. Vehicle identifiers and serial/registration numbers, including license plate numbers
- q. Full face photographic images and any comparable images

2. Is there any student information that can be released without the student's permission?

Institutions are permitted to define a class of information as "directory information." FERPA permits public disclosure of directory information without the student's consent.

3. What is directory information?

Directory information is information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed (Name, Email, College and Alternate Email).

Temple University defines directory information as:

- a. The student's name,
- b. Street address,
- c. Email address,
- d. Confirmation of enrollment status (full-time/part-time),
- e. Dates of attendance,
- f. Degree received,
- g. Awards received (*e.g.*, Dean's List),
- h. Major field of study,
- i. Participation in officially recognized activities and sports, and
- j. Weight and height of members of athletic teams.