

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student/ Consultants/Contractors</p>	<p><i>Policy Title:</i> PII Production Data Use</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 17799:2005, COBIT, NIST SP 800-68</p>	<p><i>Policy Number:</i> 9.1.4</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
--	--	--

Background

Production systems at the University of Cincinnati contain massive amounts of sensitive information. From personal data covered by Federal regulations (such as FERPA, HIPAA or GLBA) to financial information to research results, the networks and systems at UC are filled with information and data that should remain confidential. It has long been practice to use this sensitive and personal production information in non-production systems. The purpose of this policy is to ensure that UC is not exposing this information through the use of real Personally Identifiable Information (PII) or electronic Personally Identifiable Health Information (e-PHI) in development and test systems.

Policy

UC developers and various IT staff are responsible for creating and testing new applications and functionality in development and test environments. These new applications and functionalities often depend on the use of information similar to that which would occur in a production environment. The data used in the development and testing of new applications and functionality may be similar to, but not be the exact data found in production systems. The data must be used in such a way that no individual may be identified by anyone viewing it.

This policy does not apply when the test and development systems that feed into a production system and that store PII utilize the same level of physical and logical security controls as the production system that stores the same data.

Production data used in a development, test, or other non-production environment must be at least one of the following:

- Scrambled so that no individual may be identified
- Not used (made up data should be used instead)
- redacted

Audience:

This policy applies to all organizations and individuals associated with UC.

Definitions:

PII: Personally identifiable information.

Personally Identifiable Information: Information that can be traced back to a specific individual. Some types of personally identifiable information are social security numbers, name and address combinations, telephone number, credit card number or bank account number, and various combinations of these items.

Data Scrambling: Running a program against production data to shuffle data so that it is not recognizable as a unique individual.

Redacted: is the act of striking out or otherwise removing from the record or public view any sensitive, private or confidential information.

Procedure:

ISO 17799:2005	International Standards Organization for Information Security
COBIT	ISACA Audit Controls Objective for IT
NIST SP 800-68	National Institute of Standards and Technology Guide for Windows IT administrators
PCI	Payment Card Industry Standards

Related links:

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [NIST Special Publication 800-68](#)
- [Payment Card Industry Standards](#)

Phone Contacts:

UC Information Security	8-ISEC
Director, Information Security	6-9177
UC Office of the CIO	6-2228

Disciplinary Actions:

Violation of this policy may result in revocation of access to the affected system(s). Violation of this policy may also result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants and dismissal for interns and volunteers. Additionally, individuals are subject to loss of University of Cincinnati Information Resources, access privileges, civil, and in some cases criminal prosecution.