Confidentiality Agreement Requirement for Access to UD's Central Systems

Effective Date: July 2006

Approval: December 17, 2015; University President

Maintenance of Policy: Chief Information Officer

PURPOSE: The purpose of this policy is to provide guidance with regards to the access of centralized information resources during the course of employment with UD.

SCOPE: This policy applies to all UD employees – faculty, staff, student workers as well as contractors, consultants, temporaries, and/or other agents – requiring access to the information resources maintained centrally within UDit's Data Center.

POLICY:

The University of Dayton has an obligation to safeguard its information resources. In addition to information specifically categorized as confidential, non-public information that can be personally associated with an individual shall be considered confidential.

The University of Dayton grants individuals permission to its information resources. Access to resources other than one's own or those made available to the public may be necessary based upon the requirements of one's employment. Once approved, access to these additional information resources – whether University, employee, student, patient, or donor; paper or electronic - will be limited to the category or subset necessary to perform the specific requirements of one's job.

Examples of unauthorized use of an employee's permission include but are not limited to the following:

- Access to any category of university, employee, student, patient, or donor information not necessary to carry out the specific requirements of one's job.
- Access to any category of university, employee, student, patient, or donor information not necessary to carry out the specific requirements of one's job.

REFERENCE DOCUMENTS:

1. ISO 27002 2013 Sec. #9
2. Confidentiality Agreement Form

POLICY HISTORY:

Approved in its original form:
July 2006

Approved as amended:
December 17, 2015

POLICY (continued):

- Release of university, employee, student, patient, or donor information to unauthorized personnel, either internal or external, in any manner not dictated by the requirements of one's position. Unauthorized personnel may include external persons not directly affiliated with the University such as spouses, parents and legal guardians or internal personnel such as students, faculty and staff.
- Disclosure of computer credentials or allowing anyone to use the workstation at which he/she is logged into might allow unauthorized personnel to gain unauthorized access to confidential information.
- Release of more information, either in terms of unneeded records or unnecessary attributes, to an authorized individual/agency than is essential to meeting the stated purpose of an approved request.
- Access to confidential information from facilities other than the specific office and workstation provided or via any remote access applications not explicitly approved and specified during training.

In the event the employee becomes aware of unauthorized activity, whether accidental or intended, that employee should contact his/her supervisor and the applicable systems administrator.

UD employees, as defined in the scope of this policy, will be required to review this policy and sign a form for each of the administrative systems for which they require access. Copies of this form may be accessed electronically at http://www.udayton.edu/udit/_resources/documents/policies/ConfidentialityAgreementForm.pdf. In addition to the employee signing the form, the employee's supervisor and a systems administrator for the system for which he/she requires access must sign the agreement in turn prior to submitting the completed form to UDit's IT Risk Management Office for archival purposes. In those cases where the employee will serve as systems administrator on the system for which he/she seeks access, a representative of the data owner will sign as both supervisor and system manager. Completed agreements will be maintained centrally.

Access permissions required to perform a job will be rescinded immediately upon the expiration date listed on the signed confidentiality agreement, if one was provided, or upon termination of employment. To ensure accurate records are maintained, user access will be reviewed annually. System administrators should verify access permissions at that time.