NOTRE DAME OF MARYLAND UNIVERSITY

Data and Information Security Policy, Standards, Guidelines

Notre Dame of Maryland University routinely employs various measures to protect the security of its information and of its user accounts. The University seeks to maintain compliance with all Title IV, FERPA, HIPAA, e-sign security, e-commerce and PCI standards. NDMU adheres to all Gramm – Leach – Bliley Act ("GLBA") requirements. Specifically NDMU seeks to:

(i) ensure the security and confidentiality of customer records,
(ii) protect against any anticipated threats or hazards to the security of such records, and
(iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

The University is committed to engage in safe computing practices by establishing appropriate access restrictions for accounts, use of passwords, and securing backup data files. Information at NDMU is defended from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Employees

Employees of NDMU who have access to, collects, distributes, processes, protests, stores, uses, transmits, disposes of or otherwise handles customer information are required to sign a Confidentiality Agreement.

Confidentiality Agreement

The FERPA Confidentiality agreement is intended to help employees determine what information can be disclosed to non-employees or systems, as well as the relative sensitivity of information that should not be disclosed. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

ERP System Account & Password

Employees who must input data, retrieve information or submit approvals for any of the following processes must have a ERP account and personal password to access the system:

Passwords are encrypted.

ERP training includes instruction on protecting access to unauthorized persons, by logging out of open session when walking away from desk and positioning monitor away from public eyes.

ERP System Security

ERP users are given security access to information about students. Security, access and monitoring procedures are in place to ensure the continued integrity of administrative data. Users need to understand and abide by the Family Educational Rights and Privacy Act of 1974 in regards to the release of student information.

Access to protected information is restricted to people who are authorized to access the information specified in a user's security profile based on the requirements of their position.

Document Management system access is governed by permission for each user.

e-Commerce

NDMU ensures the safe handling of credit card information and adherence to the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. Credit card numbers are encrypted during transmission, and restricted to places where it is stored.