CLARION
UNIVERSITY

COURAGEOUS. *confident.* CLARION.

Information Protection Policy

Date Effective: June 25, 2014
Issued By: Center for Computing Services
Contact: Center for Computing Services, 814-393-2280

Purpose:

The purpose of this policy is to ensure the security and confidentiality of information and protect against the misuse, destruction, or loss of information especially that of a critical or confidential nature, without restricting academic freedom or complicating access to information to which the University community has a legitimate and specific need.

Policy:

It is the policy of Clarion University of Pennsylvania that all information be used in a manner that maintains an appropriate and relevant level of confidentiality and that provides sufficient assurance of its integrity in compliance with federal and state laws and State System and University policies. While the elimination of all risk is impossible, the goal of the policy is to minimize the possibility of information misuse, corruption, and loss through the adoption of reasonable policies and procedures for the University community to follow. While this policy is especially pertinent to information stored electronically, it is also intended to guide users of all information, including what is stored in other formats such as paper and video, as well as the content of confidential meetings and conversations.

Definitions:

University community - All employees and affiliates of the University.

Information - Data, regardless of format, collected, maintained, accessed, modified, or synthesized by and for members of the University community. The various forms of data include but are not limited to computer files, paper files, books, microfilm and fiche, video, and images.

Public Information - Information to which the University community has unrestricted access and for which there are no requirements of confidentiality. Public information includes, for example: directories, calendars, schedules, library books in general circulation, most meetings, and information bulletins.

Restricted Information – Information, regardless of format, which is sensitive and confidential in nature or legally constrained, and requires access only by that part of the University community with the specific need to do so. Restricted University information includes, for example, individual student grades, bills, financial aid applications, health records, personally identifiable financial information, social security numbers, driver's license numbers, and confidential personnel actions.

Responsibilities:

Access

1. Access to public information is limited only by such restrictions as circulation policies, copyright restrictions, license and contractual agreements, University policies (such as the Copyright Policy), and procedures for use.

2. Restricted information may only be accessed by those authorized members of the University community with a specific and legitimate need to know. Legitimate access does not include the freedom to "fish" (out of curiosity or other motives) for information which is restricted, if it is not specifically required to perform a job- related task or legitimate research.

Use

1. Each member of the University community is responsible for using information appropriately and within the guidelines of the University Information Protection Procedures. Appropriate use is legal, ethical, and prudent use of information so that information resources are not compromised, damaged, or misused. Inappropriate use includes releasing restricted information, accessing, erasing or modifying information without proper authorization, modifying or removing posted information without authority, and other such actions.

2. Each office responsible for University information shall identify the information it maintains, determine whether it is restricted, and implement reasonable and clear procedures for granting access only to employees with a legal, specific, and legitimate need to know. Employees must be aware of applicable restrictions on the use of information to which they have access.

3. Each member of the University community with access to restricted information is responsible for maintaining the confidentiality of that information. Each such person shall take appropriate action to ensure that the information is used and guarded appropriately. Safeguards apply to restricted information regardless of form or location and responsibilities and include, but are not limited to, the protection of computer accounts and passwords, the content of electronic messages, and storage or use on mobile devices, personal devices, or hosted cloud services,

4. Members of the University community charged with maintaining restricted information are responsible for maintaining the accuracy and integrity of that information and for determining who requires access to it. Critical information in University information systems must be backed up on a regular basis to maintain its integrity and retrievability

should it be accidentally or otherwise destroyed or lost. Individual users with critical information maintained locally, i.e., on a personal computer, on paper, or in other media, shall also take appropriate steps to ensure that valuable and confidential information not be lost, damaged, or otherwise compromised.

Oversight

1 The Information Protection Committee is responsible for the maintenance of this policy.

2. Questions regarding the applicability of the policy or appropriate access should be directed to the Associate Vice President for Computing Services.

3. Violations of this policy will be reported to the Associate Vice President for Human Resources. Violations of the policy may result in disciplinary actions up to and including separation from employment or expulsion from school in accordance with the Student Rights Handbook, applicable collective bargaining unit agreements, and/or University and PASSHE personnel policies.

4. A violation of this policy may result in criminal action if it is determined that any local, state, or federal law has been violated.

Related Documents

Acceptable Use of Information Technology Resources Policy

Digital Millennium Copyright Act Procedures

Confidentiality of Student Records

Clarion University Foundation Information System Confidentiality Policy