Information Security Policy

Section: 60.1

Section Title: General IT Guidelines

Approval Authority: Board of Trustees

Responsible Executive: Executive Vice President

Responsible Office: Office of Information Technology

Originally Issued: N/A

Revisions: 5/22/2015

Policy Summary: High Point University systems contain information that is sensitive and valuable, including: Personally Identifiable Information (PII); financial data; academic records; and other sensitive information. Some of this information is protected by local, state and federal laws or contractual agreements that prohibit unauthorized access, use or disclosure. This policy identifies data sensitivity levels that employees should use to appropriately ensure the security of information.

Reason for Policy: To ensure that sensitive and valuable information is handled responsibly and confidentially, and to guarantee sensitive information against unauthorized access.

Related Documents:

- N/A

Policy:

Purpose

High Point University systems contain information that is sensitive and valuable, including: Personally Identifiable Information (PII); financial data; academic records; and other sensitive information. Some of this information is protected by local, state and federal laws or contractual agreements that prohibit unauthorized access, use or disclosure. This policy identifies data sensitivity levels that employees should use to appropriately ensure the security of information.

Information Access Responsibilities

- Only access information needed to perform assigned or contracted job functions.
- Do not copy, destroy, release, sell, or divulge in any way University data without the express authorization of the Information Owner, or for any purposes other than the performance of assigned or contracted job functions.

- Use strong passwords in compliance with the University Password Policy, and lock or log off workstations before leaving them unattended regardless of the sensitivity level of information stored on that system.
- Protect the confidentiality, integrity and availability of all University information in whatever form it may exist (printed, computer media, exchanged in conversation, transmitted over the network, etc.)
- Destroy or render unusable any document or digital media that may contain sensitive information before discarding for any reason.
- Report any activity that you suspect may compromise sensitive information to your supervisor and/or Manager of Information Security Services within the Office of Information Technology.

These obligations continue even after you leave the University.

Information Sensitivity Levels

Information Owners are responsible to assess the Confidentiality and Integrity/Availability of their assigned datasets using the following sensitivity levels:

Confidentiality

Confidentiality refers to the authorized access to information. For the purposes of this Information Security Policy, four levels of confidentiality have been identified:

- **Public** – Information that can be shared freely with anyone.
- **Internal** – Information that can be shared only within the HPU community. Disclosure to anyone outside the University requires authorization from the appropriate Information Owner.
- **Departmental** – Information that is intended only for use within the owning department. Disclosure to anyone outside the owning department requires authorization from the appropriate Information Owner.
- **Confidential** – Information that is shared on a “need to know” basis. The Information Owner must explicitly identify who should have access to the information.

Integrity/Availability

Data Integrity refers to the accuracy of information, while Availability refers to the timely and reliable access to and use of information. For the purposes of this Information Security Policy, the two concepts are being grouped together to categorize the risk to the University should the data be corrupted or unavailable for any reason, and two categories have been identified:

- **Critical** – Information that would cause the University to suffer significant financial loss, reputational damage, or be incompliant with legal, regulatory or contractual requirements if corrupted or unavailable. Critical information **must** be stored within University Enterprise Applications, on network storage, or other suitable location(s) as identified by the Office of Information Technology where precautions can be taken to ensure the backup and recoverability of the information in the event of a catastrophic incident. **Critical information should never be stored on local hard drives or removable media devices.** Information Owners are responsible to identify Critical information and corresponding retention requirements to the Office of Information Technology.
- **Non-Critical** – Information that would pose a temporary inconvenience to the user community and/or support staff if corrupted or unavailable. In order to prevent rework or other inconveniences, Non-Critical information **should** also be stored within University Enterprise Applications, on provided network storage, or in physically secured cabinets as

deemed appropriate by the Information Owner. Non-Critical data may be stored on local computer hard drives or removable media devices with the understanding that these locations are not backed up by the Office of Information Technology and may be subject to unrecoverable loss. Information Owners are required to identify appropriate retention records for Non-Critical information stored on University systems, and to work with the Office of Information Technology to periodically discard/destroy unneeded information.

Information Owners

Sensitive information must be protected against unauthorized access, tampering or loss in accordance with applicable federal and state laws, contractual obligations, and operational significance to the University. The course instructor or head of the department on whose behalf the information is collected is to be considered the "Information Owner" of an information collection. The Information Owner may designate one or more individuals to perform the data classification duties outlined in this Policy, but the Information Owner retains responsibility.

Student Information

Information Collection	Information Owner
Applicants – Undergraduate	Vice President for Undergraduate Admissions
Applicants – Graduate	Associate Vice President for Graduate Admissions
Student Academic Records	University Registrar
Traditional Course Records	Course Instructor
Distance Education Course Records	Course Instructor
Student Health Information	Vice President for Facilities & Auxiliary Operations

Alumni and Donors

Information Collection	Information Owner
Alumni and Donor Information	Vice President for Development and Community Relations

Faculty and Staff

Information Collection	Information Owner
Applicants – Staff	Director of Human Resources
Applicants – Faculty	Director of Human Resources
Dependents and beneficiaries	Director of Human Resources
Employee health information	Director of Employee Wellness
Faculty	Director of Human Resources
Staff	Director of Human Resources
Student Employees	Director of Financial Planning

University Operations

Information Collection	Information Owner
Financial Aid	Director of Student Financial Planning
Financials	Chief Financial Officer
Library Records	Director of Library Services
Marketing and Community Relations	Vice President for Communications

Public Safety	Chief of Security
Residence Life	Vice President for Student Life
Student Accounts	Director of Student Accounts

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is any information that can be used to identify a unique person. Examples of PII include, but are not limited to: Social Security Number; Date of Birth; Place of Birth; Mother's Maiden Name; Account Numbers; Credit Card Numbers; Driver's License Numbers etc. All Personally Identifiable Information in High Point University's possession should be considered "Confidential".

Directory Information

High Point University considers the following to be "Directory Information":

Students

The Family Education Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. FERPA prohibits the disclosure of information regarding current and/or former students with the exception of "Directory Information", provided the student has not expressly objected to such disclosure. See the **High Point University FERPA Policy** for a complete listing of Student Directory Information.

Parents or Guardians

- Name
- Address
- Relationship to student

Faculty and Staff

- Name
- Dates of employment/affiliation with the University
- Office address
- Office phone number
- HPU email address
- Job title
- Department

Contractual Obligations

University employees are responsible for complying with the terms of all contracts/agreements the University has entered into that may limit the disclosure of information pertaining to the agreements or belonging to other parties. Employees are responsible to familiarize themselves with the terms of any such agreements pertaining to information they may have access to and/or to consult the appropriate Information Owner for approval before accessing or disclosing any contract information. Unless expressly directed otherwise by the appropriate Information Owner, contractual information should be considered "Confidential".
When negotiating contracts/agreements with external entities University employees should:

- Exercise care in the disclosure of University information.
- Ensure that all employees/agents of the external entity are bound to maintain confidentiality that is consistent with the University's obligations and interests.
- Ensure that all employees/agents of the external entity are contractually obligated to implement information security measures that are commensurate with the University's practices.