Huntingdon College

Information Security Policy (Version 6: 2024)

I. Purpose

The purpose of this policy is to establish standards for cyber and information security at Huntingdon College. In addition, this policy outlines responsibilities for Huntingdon College employees. Specifically, this document is intended to promote compliance with the Gramm-Leach Bliley Act (GLBA, 2002) and Part 314 - Standards For Safeguarding Customer Information [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(l)(1)(ii)]. Compliance with the GLBA is a requirement of the Federal Student Aid (FSA) Program Participation Agreement (PPA) and the Student Aid Internet Gateway (SAIG) Agreement for all postsecondary institutions.

II. Currency

The policies and procedures in this document will be reviewed for currency and appropriateness at minimum once annually by the Qualified Individual as defined herein.

Moreover, the Qualified Individual will report in writing to the College's risk management officer and the Enterprise Risk Management Committee of the Huntingdon College Board of Trustees, the overall status of the information security plan and compliance, as well as matters related to the Information Security program, including, but not limited to the most up-to-date Risk Assessment performed by the Qualified Individual. 16 CFR 314.4(i) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(i)]

III. General Definitions

A. ***Qualified Individual*** means the individual at Huntingdon College designated as in charge of overseeing, implementing, and enforcing the Information Security Policy and related program(s) and/or procedure(s). This individual is the Vice President for Technology. The Executive Vice President will provide direction and oversight of the Qualified Individual;

B. ***Personally identifiable information (PII)"***includes information that can be used to distinguish or trace an individual‘s identity either directly or indirectly through linkages with other information." [https://studentprivacy.ed.gov/content/personally-identifiable-information-pii, 07/18/19]

C. ***Storage Device*** is defined as any device which is capable of transporting or storing digital files. This includes but is not limited to such devices as flash drives, external hard drives, desktop and laptop computers, mobile devices, and cloud storage.

D. ***Encryption***" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key,

consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material."16 CFR 314.2(f) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(f)]

E. ***Multi-factor authentication***" means the authentication through verification of at least two of the following types of authentication factors:
    - Knowledge factors, such as a password;
    - Possession factors, such as a token; or
    - Inherence factors, such as biometric characteristics."
F. ***Directory Information*** is that information which constitutes a profile based on data contained within student education records that generally is not considered harmful or an invasion of privacy if released. Directory information at Huntingdon College includes:
    - Student Name
    - Address
    - Email address
    - Photograph
    - Telephone Listing
    - Date of Birth
    - Participation in officially recognized activities and sports
    - Weight and Height of athletic team members
    - Dates of attendance
    - Enrollment Status - Part-time, Full-time
    - Degree and awards received
    - Major field of study
    - Most recent previous educational agency or institution

IV. Financial Consumer Definitions

A. ***Consumer*** means an individual who obtains or has obtained a financial product or service from Huntingdon College that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.16 CFR 314.2(b)(1) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(b)(1)]

B. **Customer Information** means any record containing nonpublic personal information about a customer, whether in paper, electronic, or other form, that is handled or maintained by Huntingdon College on behalf of the College or its affiliates.16 CFR 314.2(c) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(d)]

C. ***Customer relationship*** means a continuing relationship between a consumer and Huntingdon College under which Huntingdon College provides one or more financial products or services to the consumer that are to be used primarily for personal, family,

or household purposes.16 CFR 314.2(e)(1) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(e)(1)]

D. ***Customer*** means a consumer who has a customer relationship with Huntingdon college. 16 CFR 314.2(c) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(c)]

E. ***Information System*** means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.16 CFR 314.2(j) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(j)]

F. ***Personally identifiable financial information (PIFI)*** means any information:
   (1) A consumer provides to Huntingdon College to obtain a financial product or service from Huntingdon College;
   (2) About a consumer resulting from any transaction involving a financial product or service between Huntingdon College and a consumer; or
   (3) Huntingdon College otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.
   16 CFR 314.2(n)(1) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(n)(1)'

G. ***Nonpublic personal information (NPPI)*** means:
   (1) Personally identifiable financial information; and
   (2) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
   16 CFR 314.2(l)(1) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.2(l)(1)]

V. Safeguards

(1) Access Controls

(a) Only authorized users will be granted physical or electronic access to College systems and/or physical locations.
(b) Employee access will be limited to what is needed to perform job duties.
(c) Employees shall not grant another individual access to any electronic account and/or storage device (e.g. password-sharing, MFA sharing) they have been authorized to use, without authorization by a Technology Services employee who is responsible for maintaining and granting employee access to the College's electronic systems.
(d) Employees with access to College systems and/or storage devices will take reasonable measures to ensure that such systems and/or devices are secured

from unauthorized access both at Huntingdon College and away from Huntingdon College.

(e) Access to College Information Systems and physical locations will be periodically reviewed and/or monitored.

16 CFR 314.4(c)(1) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)(1)]

(2) Storage

1. NPPI and PII will only be housed or stored in software systems and/or on storage devices administered by or provided by and approved for use by Huntingdon College.
   16 CFR 314.4(c)(2) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)(2)]
2. *Employees will not store NPPI and/or PII on non-College administered and/or non-approved College devices.*
   16 CFR 314.4(c)(2) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)(2)]
3. *Under no circumstance should NPPI and/or PII be stored on any personally-owned devices. While access to Information Systems may be permissible from personally owned devices, no NPPI and/or PII data may be stored on such devices.*
4. NPPI and PII will be stored in information system(s) in which data is encrypted at rest, unless either of these requirements are infeasible, in which case, such information may be secured using effective alternative compensating controls reviewed and approved by the Qualified Individual.
   16 CFR 314.4(c)(3) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)(3)]

(3) Transit

1. NPPI and PII will be encrypted in transit, unless this requirement is infeasible, in which case, such information may be secured using effective alternative compensating controls reviewed and approved by the Qualified Individual.
4. *Email transfer of PII is expressly prohibited.*

16 CFR 314.4(c)(3) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)(3)]

(5) Multifactor Authentication (MFA)

Multi-factor authentication will be required for any individual to gain access to NPPI or PII stored in any Information System, unless the Qualified Individual has approved in writing the use of reasonably equivalent or reasonably more secure access controls.

16 CFR 314.4(c)(5) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(c)(5)]

VI. Change Management

(1) Acquisition of Technology Hardware and/or Software

- *Employees must submit devices and/or software intended to store, process, or transmit NPPI and/or PII for approval by the Qualified Individual before acquisition of or use for such purposes.*
- *All technology hardware purchases in excess of $500.00 must be approved by the Qualified Individual.*
- *Each software and/or storage device (hardware) contract must be reviewed by appropriate College officials to determine compliance with College Policies and Procedures.* Items for consideration may include as appropriate to the intended use and type(s) of data which will be stored and/or transmitted:
  - Whether reasonable data protection measures exist.
  - Whether cyber-insurance is kept on the part of the third party.
  - Whether data backup procedures are followed by the third party.
  - Whether required accessibility features commensurate with currently available accessibility technologies are present.

(2) Development and Administration of Software

- *Employees must submit any applications developed by Huntingdon College for transmitting NPPI and/or PII for review and approval by the Qualified Individual before developing and/or using such applications.*
- *For any software managed by Technology services, any substantive software setting(s) and/or configuration changes and/or adjustments shall be approved by the Qualified Individual.*

(3) Disposal of Hardware

Employees must return any College-issued devices no longer intended for employee use to Technology Services, which will use reasonable measures to ensure secure reissuance or secure disposal of any such devices.

(4) NPPI/PII

The copying, downloading, FTP transfer, collection of, or otherwise duplicating of PII and/or NPPI data on a computer, website, USB device, or other such mobile storage device for purposes other than backup by authorized personnel is prohibited.

(5) Surveys

The Qualified Individual (Vice President for Technology) must approve the collection of PII or other potentially sensitive information, (definitely including, but not limited to Social Security Number, Government ID, Driver's License number or copy, Passport information or copy, and personal tax information) to ensure appropriate security measures are in place. Surveys and/or other data collection methods or forms must be approved by a senior employee in the area to which the data primarily pertains:

- *Academics: Chief Academic Officer*
- *Students: Dean of Students*
- *IRB: Qualified Individual*
- *Employees: Risk Manager*
- *All Others: Risk Manager*

Data collected and/or compiled for distribution to other entities must be approved by the Qualified Individual before distribution.

VIII. Training

(1) *Information Security Training relevant to current risks will be completed once per year, and all active employees at the time of the training will be required to participate, though any employee on active military duty at the time of Security Training may have this requirement waived.*

(2) Employees in Technology Services will take part in periodic and/or ongoing training and/or professional development and/or research relevant to this policy.

IX. Enforcement

- Employees will be required to sign Non-Disclosure documentation.
- Any employee found to have violated this policy may be subject to disciplinary action.

X. Risk Assessment

A risk assessment addressing reasonably foreseeable internal and external risks to information security will be completed at least annually by the Qualified Individual. This shall include at minimum:

"

(i) Criteria for the evaluation and categorization of identified security risks or threats;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of the College's information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks."

16 CFR 314.4(b)(1) [https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314#p-314.4(b)(1)]

XI. Network Security Monitoring

Huntingdon College contracts with a network provider whose services include monitoring of security and performance of the College's network which is used for business purposes.

XII. Disclaimers

(1) *Huntingdon College is not responsible for the confidentiality, integrity, and/or availability of any information uploaded to or transmitted via any of the College's systems and/or devices, if that information is not related to College Operations.*

II. Document Review and/or Update History

Note: this documentation began being recorded here in June 2023.

- May 2023
- June 2023
- July 2024