Version: May 1, 2013

Nazareth College Policy

Information Security Policy

Table of Contents

1. Policy Name: Information Security Policy

2. Rationale / Purpose

Nazareth College creates, collects, maintains, uses and transmits confidential information, including Personally Identifiable Information (PII) relating to individuals associated with the College, including, but not limited to, applicants, students, parents, alumni, employees and vendors. The College is committed to protecting the confidentiality, integrity, and availability of this information against inappropriate access and use. To that end, the Information Security Group (ISG) was established in 2011 to partner with the Nazareth community to provide ongoing proactive security policies, procedures and education and to promote a general culture of security awareness.

This policy and associated procedures and standards provide direction for information security in accordance with College requirements and relevant laws and regulations. Nazareth College information security practices are designed to promote and encourage appropriate use of information assets. They are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the College's core mission and campus academic and administrative purposes.

In adopting this Policy, the College strives to help all College community members to understand the definition of confidential information and their obligations and individual responsibilities. The College will provide appropriate training and education that will enable the College community to comply with the intent and the specifications laid out by the Policy.

3. Policy Statement

Members of the College community will employ reasonable, practical and appropriate administrative, technical, physical and procedural safeguards to protect the integrity, confidentiality and security of all confidential information, in particular Personally Identifiable Information (PII). In recent years, state and federal regulations have mandated specific protections for different types of information, including SSN. The New York State Breach Law and the breach laws of other states define PII, provide guidelines governing PII and outline action to take in case of a data breach. The specific data elements considered PII are defined later in this document, in section 4.2

4. Scope and Definitions

4.1 Scope

This Policy applies to all members of the Nazareth College community, including employees (both faculty and staff), student workers, and other individuals such as service contractors, *vendors and consultants, who have a relationship with the College and whose responsibilities give them access to confidential information. This Policy applies to the access, use, storage, transmittal and destruction of confidential information belonging to any individual, regardless of the media in which it occurs, including both paper and electronic formats.*

4.2 Information Security Categories

Confidential information is categorized according to the data's confidentiality impact, so that appropriate safeguards can be applied. The confidentiality impact level- High (Level 1), Moderate (Level 2) or Low (Level 3)- indicates the potential harm that could result to the individuals and/or the College if confidential information were inappropriately accessed, used, or disclosed. Each of the three security categories, or levels, has accompanying sets of measures. Level 1 has the tightest security controls to protect the most sensitive, high-risk confidential data. Level 2 measures protect additional confidential data. Level 3 controls protect the College's enterprise-specific data.

High Risk - Level 1: High Risk Confidential Information (HRCI)

The confidentiality impact is HIGH if the loss of confidentiality, integrity, or availability could have a severe or catastrophic adverse effect on College operations, organizational assets, or individuals.[1]

- *High Risk Categories*

  Information is classified as high risk, either because the exposure of this information can cause harm or because the information is specifically protected under law or under contract. Extra care must be taken to protect high-risk confidential information in both electronic and paper form. High Risk Confidential Information includes Personally Identifiable Information (PII) and personally identifiable medical information.

- *Permission to access High Risk Confidential Information (HRCI)*

  Permission to access HRCI is tied to position definition and responsibilities. Any person whose position does not grant access to HRCI must obtain permission from ISG.

- *Personally Identifiable Information (PII)*

  Personally Identifiable Information is information that can be used to distinguish or trace an individual's identity. A data breach is defined as access to personal information, such as name, in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:[2]

[1] "Guide to Protecting the Confidentiality of Personally Identifiable Information", National Institute of Standards and Technology (NIST), US Dept of Commerce, April 2010.

[2] http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$STT208$$@TXSTT0208+&LIST=SEA3+&BROWSER=EXPLORER+&TOKEN=52890818+&TARGET=VIEW

- *Date of Birth*
- *Social Security Number*
- *Bank or brokerage account number or code*
- *Credit card number or code*
- *Debit card number + access code*
- *Driver's license number or non-driver photo ID card number*
- *Computer system password*
- *Protected Health Information*
- *Educational Records*

Moderate - Level 2: Confidential Information (CI)

The confidentiality impact is MODERATE if the loss of confidentiality, integrity, or availability could have a serious adverse effect on organizational operations, organizational assets, or individuals.

- *Confidential Information*

  Information about a person or an entity that, if disclosed, could reasonably be expected to place the person or College at risk of criminal or civil liability, or to be damaging to financial standing, employability, reputation or other interests. Confidential Information includes non-public personal information about an individual.

- *Examples*

  Examples of Confidential Information include, but are not limited to, the following:
  - *Employee salary, benefit and other HR information*
  - *Personal cell phone numbers*
  - *Unpublished College financial statements and development plans*
  - *Non-public personal and financial information about applicants, students, alumni, corporations and donors*
  - *Information regarding College information and facilities security systems*

- *Permission to access Confidential Information (CI)*

  Permission to access Confidential Information is tied to position definition and responsibilities. Any person whose position does not grant access to CI must get authority from the appropriate Data Custodian. The list of Data Custodians is appended to the corresponding Information Security Procedures document.

Low - Level 3: Enterprise Data.

The confidentiality impact is LOW if the loss of confidentiality, integrity, or availability could have a limited adverse effect on organizational operations, organizational assets, or individuals.

- *Nazareth College maintains records for its applicants, students, alumni, donors, employees and business associates. All employees and contractors who have access to enterprise data are responsible for maintaining the availability, integrity and privacy of such data.*

4.3 Data Breach

- *Definition.*
  Data Breach refers to an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information, as defined in the previous section. Good faith acquisition of personal information by an employee or agent of the College for the purposes of the College is not a breach of the security of the system, if the private information is not used or subject to unauthorized disclosure.[3]

- *Reporting a Data Breach.*
  - *If it becomes known or suspected that College confidential information (HRCI or CI) may have been acquired or used by an unauthorized person or for an unauthorized purpose, the matter should be immediately reported to the Director of Campus Safety.*
  - *Under New York law, Nazareth must notify affected New York residents and state officials as soon as practicable if a resident's "personal information" has been acquired or used by an unauthorized person or used for an unauthorized purpose. Reportable security breaches of this kind may include unauthorized access to a system that stores confidential information, or the loss or theft of a system or a physical record that contains confidential information, or cases where computers or personal devices (ipads, smartphone, laptops) have been hacked, lost or stolen or passwords have been compromised.*
  - *Possible breaches must be reported as soon as possible after becoming aware of the possible breach to the Director of Campus Safety. Reporting should not be delayed in order to collect more information, to determine if a breach has actually occurred, or to determine what specific personal information was actually involved.*

5. Related Policies and Information

- *Nasareth College Information Security Procedures*
- *Nazareth College Email Policy*
- *Nazareth College FERPA Policy(http://www.naz.edu/registrar/ferpa-policy)*
- *Nazareth College Data Standards*
- *HIPAA Privacy Rules, Staff Policy Manual Amendment #11 (http://www.naz.edu/human-resources/documents/employee-manual)*
- *Nazareth College Six Best Practices Data Security*

[3] NYS "State Technology Law" 208

6. Policy Changes

Policies and procedures are subject to review and may be modified at any time. Policies and procedures will be formally reviewed regularly by Information Technology Services(ITS) and Information Security Group(ISG), or in conjunction with significant system upgrades, whichever occurs sooner. Final approval for significant changes will come from Senior Staff.

Approval Date: July 7, 2014
Effective Date: July 7, 2014
Approval Authority: Information Security Group