Institutional Data Governance Policy

Effective Date: TBD
Revision Date: 1/31/2019

DOCUMENT CONTROL

Document Title	Institutional Data Governance Policy		
Summary:	This document defines the policies of Holy Names University regarding data governance.		
Date of Issue:	TBD		
Version:	Version 1.0		
Contact Officer:	Institution Data Governance Executive Director		
Relevant References:	HNU Internal References: Human Resources, Policies		
Change History	Version	Who	What
	2.5	Herrera, Francisco Sticka, Stephen	1/31/2019: Included description of General Data Protection Regulation (GDPR) policy.

INTRODUCTION

Background

Institutional data are assets maintained to support Holy Names University's central mission of academic excellence and service. To support effective and innovative management, institutional data must be accessible, must correctly represent the information intended, and must be easily integrated across Holy Names University's information systems to support the organization's strategic plans.

The Holy Names University executive leadership team recognizes the value-added benefits of being able to aggregate information across multiple complex systems and business processes that enable Holy Names University to be an excellent University and leader. The Data Governance Committee is responsible for establishing data governance policies, procedures, standards, and guidelines for ensuring maximum value of our data.

Objectives

The Data Governance Policy addresses data governance structures and includes sections on data access, data usage and data integrity and integration. Adherence to the data governance policy and procedures shall;

- Establish appropriate responsibility for the management of institutional data as an institutional asset.
- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.
- Improve the security of the data, including confidentiality and protection from loss.
- Improve the integrity of the data, resulting in greater accuracy, timeliness and quality of information for decision-making.
- Establish standard definitions for key institutional data to promote data integrity and consistency.

The purpose of data governance is to develop institution-wide policies and procedures that ensure that our data meet these objectives within and across our administrative or academic data systems.

Scope

For the purpose of this policy, the term "Holy Names University" includes the following areas:

- Academic Affairs
- Administration
- Admissions
- Athletics
- Campus Services
- Development & Alumni Relations

- Finance
- Financial Aid Office
- Human Resources
- Information Technology
- Marketing
- Mission and Ministry
- Registrar
- Student Accounts
- Student Affairs

“Institutional Data” refers to data elements that are aggregated into metrics relevant to operations, plan ning, or management of any unit at Holy Names University that is reported to Holy Names University’s Board of Trustees, federal and state organizations, generally referenced or required for use by more than one organizational unit, or included in official administrative reporting.

Policy applies to anyone engaged with Holy Names University by employment or contract that creates, manages or reports these data referenced in scope above on behalf of Holy Names University, or relies on these data for decision making and planning.

Who Should Read This Policy

All Holy Names University employees who use data, regardless of the form of storage or presentation. All senior administrators have the responsibility to understand and implement this policy, including, as necessary, the adoption of specific procedures for their respective areas in furtherance of and in accordance to this policy.

POLICY

Data Access

One purpose of the data governance policy is to ensure that employees have appropriate access to institutional data and information. While recognizing the institution’s responsibility for the security of data, the procedures established to protect that data must not interfere unduly with the efficient conduct of our business. The policy applies to all uses of Holy Names University data covered by the scope of this policy regardless of the offices or format in which the data reside.

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuses, misinterpretation, inaccuracies, and unnecessary restrictions to its access.

The institution will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant Data Steward to have an appropriate access level. HNU IT will provide the technology framework for data access to be provisioned. The Data Stewards are responsible for ensuring the access levels are appropriate. Read-

only access to administrative information may be provided to employees for the support of institutional business without unnecessary difficulties/restrictions.

Any employee or non-employee denied access may appeal the denial to the Data Governance Committee. Escalation to the executive management should only be pursued if the Data Governance Committee decision needs to be appealed.

Data Usage

Another purpose of data governance policy is to ensure that institutional data are not misused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the Data Steward.

Holy Names University personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of update and dissemination.

Update

Authority to update data that is reported as key institutional data shall be granted by the appropriate Data Steward only to personnel whose job duties specify and require responsibility for data update. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with Holy Names University's desire to provide excellent service to faculty, staff, students, and other constituents. Data Stewards shall ensure that adequate internal controls and/or change management procedures are in place to manage ‘updates’ to key institutional data, their definitions and processes.

Dissemination

Dissemination of data must be controlled in accordance with the security practices set forth by the Data Stewards. Appropriate use must be considered before sensitive data are distributed. Unauthorized dissemination of data to either internal/external personnel is a violation of this policy.

Data Integration

Data integration refers to the ability of data to be assimilated across information systems. It is contingent upon the integrity of the data and the development of a data model, corresponding data structures, and domains. Data model designs should focus on utilizing IT Industry best-practice methodologies in order to streamline how data is integrated when applicable.

System-to-system interfaces are a standard practice to move data from one system to another in order to streamline processes that extend across systems and contribute to using data efficiently and effectively.

Operational processes often require systems to exchange information. System interfaces are often

developed between systems to facilitate the exchange of such information. The systems that exchange information fall into two broad categories:

- Internal – Systems that are implemented within the Holy Names University computer systems network. They can either be procured, procured but modified, or custom developed products.
- External – Systems that do not reside on a Holy Names University computer network. These systems are hosted by vendors and/or through sub-contracts managed by vendors.

Downloading of individually identifiable data from central systems to electronic files for the purpose of uploading or connecting the data to non-central systems (e.g., shadow systems, external vendors) without the knowledge of the Data Steward is prohibited. This practice is not supported and introduces risks associated with data integrity, security, and long-term sustainability of information systems that may not be mitigated due to the nature of the practice. Departments and/or personnel responsible for these practices that are found to be in violation of this policy, may result in disciplinary actions up to and including dismissal from employment consistent with University Policy.

Approval by the Data Steward is specific to each request. Data granted for one purpose is not universally granted for all purposes. Each new use case must be approved by the Data Steward in a new request or an amendment to the original request, even if you already have the data.

Documented agreements regarding data use, retention, and responsibility should exist with the Data Stewards (and vendors in the case of data integration with external entities) of the systems providing and utilizing data. Data extraction practices that are already in use should be registered and documented agreement developed with the appropriate Data Steward member.

Data Integrity

Data systems and/or processes that are involved in the creation of institutional reports should incorporate data integrity and validation rules that ensure the highest levels of data integrity are achieved. Validation rules within data systems may need to include reconciliation routines (checksums, hash totals, record counts) to ensure that software performance meets expected outcomes. Data verification programs such as consistency and reasonableness checks shall be implemented to identify data tampering, errors, and omissions.

RESPONSIBILITIES

Data Governance Structure

The function of applying policies, standards, guidelines, and tools to manage the institution's information resources is termed data governance. Responsibility for the activities of data governance is shared among the roles listed below. Descriptions of roles and responsibilities below provide the framework of how data governance will be implemented and maintained.

Current membership of each committee and role can be found at: www.hnu.edu/datagovernance

President's Cabinet

The President's Cabinet are senior Holy Names University officials who are responsible for setting the overall prioritization for institutional business process redesign projects; communicating process transformation priorities across the institution; ensuring project resources are available and adequate to meet established time lines; bringing clarity whenever necessary to project, process and data work; approving data governance policy; appointing members of institutional data governance committees. The President's Cabinet will review and make approval decisions on policies presented by the Data Governance Committee.

Data Governance Committee (DGC)

The Data Governance Committee (DGC) committee is the body responsible for developing and submitting to the President's Cabinet for approval the data governance policy on data access, data usage, data integrity and integration, and data security, proposing prioritization of business intelligence work; ensuring that work plans are established and met; and, reporting up to the President's Cabinet on project status and seeking input on projects that have broad institutional implications related to business intelligence and data. Assignment of personnel to the key roles listed below requires consensus within the DGC committee.

Membership

The President's Cabinet are responsible for the Data Governance Committee (DGC) committee membership. Changes to the DGC membership must be nominated to the DGC. Upon approval, the President's Cabinet will review and provide an approval decision based on the recommendation.

Data Architecture, Standards, & Reporting Committee

The Data Architecture, Standards, & Reporting committee is a sub-committee to the DGC. This committee designs the technology architecture to support the reporting needs, carries out policies set by the DGC, responsible for maintaining technology product roadmaps (software & hardware) necessary to support the current and future state reporting requirements, addresses data quality and integrity, and sets forth data standardization and standard reporting practices into the institutional reporting environments.

Membership

The Data Governance Committee (DGC) is responsible for the Data Architecture, Standards, & Reporting committee membership. Changes to the membership must be nominated to the DGC. The DGC will review and provide an approval decision based on the recommendation.

Data Stewards

Data Stewards are appointed by functional area senior leadership to develop data centric policies and carry out the overall administrative data security policies. Data Stewards are responsible for making

known the rules and procedures to safeguard the data from unauthorized access and abuse. They authorize the use of data within their functional area and monitor to verify appropriate data access. They assist institutional data users by providing appropriate documentation and training to support institutional data needs.

Data Managers

Data Managers coordinate and manage the data in the business process that results in the data adhering to Holy Names University standards. Once data have entered the system, there is a process by which they are validated, transmitted, stored, and archived. The capture and checking are typically based on a functional process or business process. This data manager role oversees adherence to the business process and in some cases develops the process. While there may be several data managers, the Data Stewards will appoint one as primary for each application.

Data Reporters

Data Reporters are individuals within the institution who have an intricate understanding of the data in their area. They establish reporting procedures for institutional data, which may include recommending changes to data entry practices. They are responsible for implementing the decisions of the Data Stewards in functional areas, assuring that census, backup, and retention plans are implemented according to defined needs. Because data reporters have a hands-on role with data, they monitor or oversee monitoring of data quality.

Functional Security Leads

The functional security leads are responsible for allowing access within the rules and standards set by the Data Steward for their area. The security leads should work with the Data Stewards for each area to document the agreed upon procedures that will be followed to administer security access.

It is the responsibility of the functional security leads to routinely monitor access and ensure that access levels are up to date.

PROCESS

Data Governance Standards

The purpose of establishing standards is to ensure that institutional data have a high degree of integrity and that key data elements can be integrated across functional units and electronic systems so that faculty, staff, and management may rely on data for information and decision support.

Institutional data will be consistently interpreted and clearly documented, according to the best practices agreed upon by the DGC, and it will have documented values in all Holy Names University systems. It is the responsibility of each Data Steward to ensure the correctness of the data values for the elements within their charge.

Institutional data are defined as data that are maintained in support of a functional unit's operation and meet one or more of the following criteria:

- The data elements are key fields, that is, integration of information requires the data element;
- The institution must ensure the integrity of the data to comply with internal and external administrative reporting requirements, including institutional planning efforts;
- The data are reported on or used in official administrative report
- A broad cross section of users require the data.

It is the responsibility of each Data Steward, in conjunction with the DGC, to determine which core data elements are part of our institutional data.

Documentation (metadata) on institutional data will be maintained within an institutional repository according to specifications provided by the Data Standards & Reporting Committee. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within an academic or fiscal calendar.

All employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate Data Stewards or any member of the DGC.

Communicating Data Governance Standards

The Data Architecture, Standards, & Reporting Committee is responsible for establishing data standardization and standard reporting practices. The committee will obtain approval from the Data Governance Committee (DGC) when standards are developed and/or modified. A central repository will be maintained and should be referenced for specific guidelines and decision outcomes related to data governance as set forth within this policy. The repository of reporting standards, documented institutional data, and key decisions can be found at: www.hnu.edu/datagovernance

OVERSIGHT

Penalties for deliberate violations of this policy will be adjudicated in accordance with applicable disciplinary policies and procedures as stated in University Policy.

Data Protection Privacy Notice

- **General Data Protection Regulation (GDPR)**

INTRODUCTION

Effective May 25, 2018, in the context of certain activities the European Union (EU) General Data Protection Regulation (GDPR) will apply to the processing of personal data of individuals residing in the European Union and apply to the processing of personal data by controllers and processors in the territorial jurisdiction of the European Union, regardless of whether the processing takes place in the European Union or not.

Holy Names University (the "University", "we", "our", or "us") is committed to safeguarding personal data that is submitted to the University, either directly or indirectly by use of our websites or other services, by you. The University is a data controller or data processor when conducting official business and research activities, including behavior monitoring, in the applicable territorial jurisdiction and therefore, must comply with the GDPR. This GDPR-Privacy Notice governs the capture, use, transfer, and storage of your personal data, as defined under the GDPR.

COLLECTION OF PERSONAL DATA

Under the GDPR, personal data is any information relating to an identified or identifiable natural person ("data subject"), which identifies or relates to you, either on its own or in conjunction with other information held by the University, such as a name, an identification number, location data, online identifier (e.g., IP addresses and device IDs). Personal data can include name, job title, and date of birth, address, telephone number, and email address. There are also special categories of personal data (sensitive personal data) that relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sexual orientation.

The University collects sensitive personal data if submitted by you as a voluntary response to inquiries by the University or our third-party service providers, as our data processors.

The University collects and processes personal data about you for the purposes described below. Personal data will be treated as Private Information under the University's General Privacy Policy. The University shall limit the collection of personal data, as defined under the GDPR, to only that information that is strictly necessary and lawful to accomplish a lawful purpose or legitimate interest as permitted under the GDPR.

PURPOSES AND USE OF INFORMATION

In order to fulfill the University's mission, the University needs to collect and process personal data relating to current, past, and prospective students, employees, volunteer affiliates, alumni and supports, suppliers, research subjects, international patients, exchange visitors and research learners and others

with whom it conducts official business. Personal data will only be disclosed in accordance with the GDPR in force at the time. If your consent is required before we can share your personal data we will contact you to request the specific consent required.

If we are collecting or processing sensitive personal data, as defined in the GDPR, additional safeguards will be put in place in accordance with the University's Data Classification and Handling Policy. We may use and disclose fully anonymized data without limitation. When requesting your personal data, we will identify the legal bases for processing your personal data. If the legal basis for processing your personal data is based on your consent, we will contact you if or when further processing for other purposes is intended. When necessary to transfer or share your personal data to organizations or agencies based outside the European Union, we will ensure appropriate and suitable safeguards are in place in accordance with the GPDR.

More information relating to the conditions for processing your personal data can be obtained by contacting the University's Data Protection Officer.

RETENTION AND DESTRUCTION OF YOUR INFORMATION

Your personal data will be retained by the University, its affiliated entities, or its third party service providers in accordance with the applicable federal and state laws, and the applicable retention periods in the University's Records Retention Schedules or the Research Record Management, Disposition and Retention Policy for HNU, as applicable.

Your personal data will be destroyed upon your request or after the expiration of the applicable retention period, whichever is later. The manner of destruction shall be appropriate to preserve and ensure the confidentiality of your personal data given the level of sensitivity, value and criticality to the University. Appropriate data will be retained permanently to ensure your educational record is held on file for all lawful purposes.

YOUR RIGHTS

You have a number of rights under the GDPR. These include the rights to request access to, a copy of, rectification, restriction in the use of, erasure of your personal data and portability. The erasure of your personal data is also subject to the University Record Retention Schedule or the Research Record Management, Disposition and Retention Policy for HNU, as applicable, and the Student Records Policy. You also have the right to withdraw consent to the use of your personal data.

You may exercise these rights by contacting:

Data Protection Officer, at 510.436.1648 or via e-mail at jcastillo@hnu.edu

RESOURCES

- Holy Names University Policies
  - Electronic Communications and Information Technology Resources
    - Policies
  - Holy Names University Computing Privileges and Responsibilities – Acceptable Use Policy
    - http://www.hnu.edu/info/computing-aup/
  - Related Federal Regulations
    - Family Educational Rights and Privacy Act (FERPA)
      - http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
    - Health Insurance Portability and Accountability Act (HIPAA)
      - http://www.hhs.gov/ocr/privacy/

CONTACTS

Data Governance Committee Co-Directors:

Francisco Herrera, Director of Institutional Research, herrera@hnu.edu

Stephen Sticka, University Registrar, sticka@hnu.edu

DEFINITIONS

Data Element

A single data item. For example, last name is a data element.

Data Dictionary

A reference tool, which provides a description of all the core institutional data elements.

Data Dissemination

The distribution of data to either internal or external stakeholders. Included in dissemination is the sending of data to external entities including vendors that provide services for Holy Names University.

Data Integrity

The qualities of reliability and accuracy of data values that permit the institution to have dependable data on which to make plans, projections and decisions. Data integrity contributes to the efficient operation of the institution by supporting quality customer service to students, faculty and employees, and helping the institution remain competitive.

Data Integration

The ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

Data Model

A diagrammatic representation of the objects and their properties that are needed within an organization to accomplish its mission. Sometimes represented as an ER (entity-relationship) diagram or a data flow diagram.

Data Value

The set of values that each data element can have. For example, ABD, BSN, MBA, and CPSY are a selection of values of the data element named school.

Institutional Data

The data elements that are aggregated into metrics relevant to operations, planning, or management of any unit at Holy Names University, that are reported to Holy Names University's Board of Trust, federal and state organizations, generally referenced or required for use by more than one organizational unit, or included in official administrative reporting.

Metadata Repository

Information about the data in an organization's electronic systems. It is used to catalog the data elements and to enable software development tools and operational systems to assess the data. Data Stewards add interpretive information to the repository so that the meaning of each element is clear, and can be use consistently across all systems. Data dictionaries are built from the repository.