Establishing Data Governance Practices at William Paterson University

Introduction

Data governance is critical to the successful implementation of William Paterson University's strategic plan. At the core of a successful implementation is the need for an integrated data-driven planning process. The University is poised to take the next critical step of viewing its data as a University-wide asset that is formally managed so that University-defined planning, research and operational needs are met in an accurate and timely manner. An acknowledged way to achieve an integrated information world is through data governance policies and practices (see references). In addition to the internal need for data quality, an equally pressing motivation to establish data governance procedures comes from external regulatory and legal requirements.

The following ideas and suggestions for establishing a data governance process at WPU heavily rely upon Virginia Polytechnic Institute and State University and the University of Nevada Las Vegas' (UNLV) data governance documentation and plans.

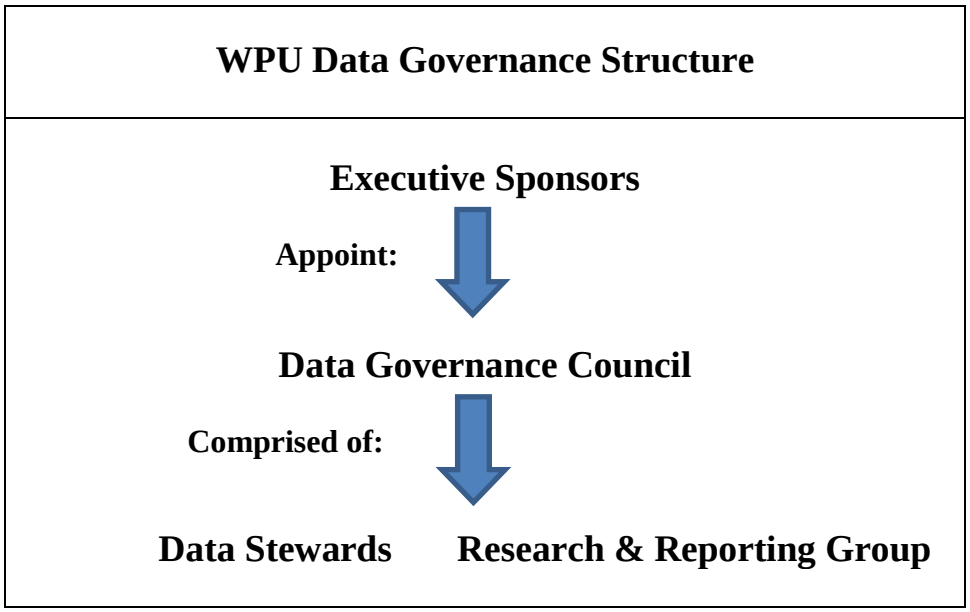
William Paterson University's Data Governance Policy

This policy establishes uniform data management standards and identifies the shared responsibilities for assuring that the University's Enterprise Data Base has quality and that it efficiently and effectively serves the needs of William Paterson University. This policy applies to those data that are critical to the administration of the University, regardless of whether the data are used or maintained by administrative or academic units.

1.0 Objectives of Data Governance

1. To recognize and treat "Enterprise" data as a University resource that does not belong to any one area or individual. This is data that is shared, or potentially shared, across business areas and must meet all users' needs and includes, for example, data about students, courses, employees, finances.
2. To ensure the quality of the data resulting in greater accuracy, timeliness, and a clear understanding of the data.
3. To ensure the security of the data, including confidentiality and protection from loss. Appropriate backups and disaster recovery measures shall be administered and deployed for all Enterprise data.
4. To ensure the ease of use of Enterprise data, sufficient information will be available for data users to accurately understand and interpret the data. Enterprise data and information about that data (meta-data) will be readily accessible to all, except where a data element(s) is determined to be restricted. When restrictions are made, business stewards of the Enterprise data are accountable for defining specific individuals and levels of access privileges that are to be enabled. Information Security will be responsible for the implementation of proper security controls.
5. To establish appropriate responsibility for the management of the University data, data stewards will be appointed by the executive sponsors. Data Stewards are those individuals ultimately responsible for the definition, management, control, quality or maintenance of a departmental or Enterprise data resource. Individuals designated as stewards will have their duties incorporated into their job descriptions.
6. To clearly document and manage Enterprise data.

2.0 Data Management Structure: Roles and Responsibilities



2.1 **Executive Sponsors** are senior University officials with planning and policy-level responsibility and accountability for data within their functional areas. By understanding the information needs of the overall institution, they articulate for the University how data can be used strategically to meet the University's mission and goals. Their vision is articulated and realized through the Information Technology Plan. As a group they also are responsible for overseeing the establishment of any data management policies and procedures and for the assignment of data stewards.

Membership:
Provost or designee Associate Provost
Director of Institutional Research and Assessment
Vice President Enrollment Management
Vice President Administration and Finance
Chief Information Officer
Vice President Student Development or designee Associate Vice President Student Development
Vice President Institutional Advancement
Executive Assistant to the President

2.2 **Data Stewards** are University directors or associate directors, who oversee the capture, maintenance and dissemination of data for a particular operation. Key Data Stewards are appointed by the respective Executive Sponsors and work in unison with those on the Research and Reporting group. They will meet regularly and are guided by the charge to data stewards from the Executive Sponsors.

Membership:
Executive Director Enrollment Management and Technology (divisional coordinator)
Undergraduate Admissions
Graduate Admissions
Registrar
Financial Aid

Student Enrollment Services
Student Accounts
Associate Director Budget
Human Resources
Information Technology Programmers
Institutional Research and Assessment
Testing Office
Residence Life
Transfer Programs and Special Sessions
Alumni/Advancement
Educational Enrollment and Certification

2.3 **Data Managers** are staff in a functional area with day-to-day responsibilities for the capture, maintenance, and dissemination of data for a particular operation. *A Data Manager generally reports to a Data Steward*. The data management activities assigned to a Data Manager may be specified in this policy, in position descriptions or delegated by a Data Steward.

Membership: The appropriate functional area staff is defined by the data steward.

2.4 **Data Experts** are operational managers in a functional area with day-to-day responsibilities for managing business processes and following the business rules for the production transaction systems. *A Data Expert generally reports to a Data Steward*. The data management activities assigned to a Data Expert may be specified in this policy or delegated by a Data Steward.

Membership: The appropriate functional area staff is defined by the data steward.

2.5 **The Research and Reporting Group** are data users who have specific data needs because they must meet external and internal research reporting requirements often for planning purposes. The Data Stewards and the Research and Reporting Group will work together as the Data Governance Council to ensure data meets all information needs: external reporting, research, planning and operational.

Membership:
Associate Director Institutional Research and Assessment, **Co-Chair**
Associate Director Enterprise Information Systems, **Co-Chair**
Enrollment Management
Executive Director Enrollment Management and Technology (Area Coordinator)
Undergraduate Admissions
Graduate Admissions and Enrollment Services
Registrar
Financial Aid
Student Enrollment Services
Academic Affairs
Transfer Programs and Special Sessions
Academic Development
Educational Enrollment and Certification
Administration and Finance
Budget
Human Resources
Campus Police

Controller
Student Development
Hospitality Services
Counseling
Divisional representative
Information Technology
Programmers as needed
Alumni/Advancement

2.6 **Data Users** are individuals who access university data in order to perform their assigned duties or to fulfill their role in the university community. Data Users are responsible for protecting their access privileges and for proper use of the university data they access.

2.7 **Information Resource Management** is a team within Information Technology consisting of database management and security system specialists. The Information Resource Management team works cooperatively with the Data Stewards, Data Experts, and Data Managers to specify, implement, and maintain appropriate security controls and authorized access for Data Users.

2.8 **Information Warehousing and Access** is a team within Information Technology consisting of data archiving and reporting specialists. Information Warehousing Access works cooperatively with the university community to implement a data warehousing system that collects, structures, and delivers university data to support timely, effective decision-making. As information technology moves the University towards a distributive reporting environment, the executive sponsors recognizes that new skill areas will be needed in functional areas. This may take the form of new employees or a redistribution of time of already hired employees. Training in the software necessary to produce summary and statistical information will be the responsibility of information technology.

2.9 **University Information Technology Security Officer.** The function within Information Technology that is responsible for maintaining a plan for security policies and practices and for keeping abreast of security related issues internally within the university community and externally throughout the information technology marketplace.

3.0 Data Management Principles

3.1 **Data Ownership.** The University Enterprise Database System (UEDS) is a university resource; individual units or departments may have stewardship responsibilities for portions of the enterprise data.

3.2 **Data Definition.** Data Stewards and Data Experts provide data descriptions so Data Managers and Data Users know what shareable data are available, what the data mean, and how to access and process the data. Data definitions may be stored in an integrated or complementary database known as a ***Metadata Repository***. The University uses iData Datacookbook for Data definitions documentation which are modified only through procedures established by the Data Governance Council and periodically reviewed for currency.

3.3 Data Administration. The function of applying formal guidelines and tools to manage the university's information resource is termed data administration. Responsibility for data administration activities is shared among the members of the Data Governance Council—Data Stewards, Research and Reporting group members, Data Experts, Data Managers and Information Technology programmers/staff. Where information is shared among systems, Information Technology will document the process and identify the responsibilities.

3.4 Data Integration Model. The Data Stewards, or designated Data Experts and Data Managers, collaborate to establish and maintain a university-wide Data Integration Model that describes all major data entities of the University Enterprise Database and the relationships among those data entities. Included in the model are the linkages among data collected or maintained by the various organizational units of the university. The Information Warehousing and Access (IWA) area of Information Technology provides expertise and software tools for data modeling. An integrated data model acknowledges the need for software to be vetted through Information Technology.

3.5 Security Administration. The function of specifying, implementing, and maintaining access control to assure that Data Users have the appropriate authorized access needed to perform assigned duties or to fulfill university roles. The ITSecurity and Data Base Administrators team of the Information Technology organization, Data Stewards, Data Experts, and Data Managers shares responsibility for security administration activities.

3.6 System Administration. The function of maintaining and operating hardware and software platforms is termed system administration. Responsibility for system administration activities belongs to Information Technology or to other organizations as deemed appropriate by Information Technology.

4.0 Procedures

4.1 Data Administration. This section describes the data administration activities that are the ultimate responsibility of the Data Steward for a particular functional area. These activities may be delegated to Data Experts and Data Managers as deemed appropriate. (See also the ***List of Data Steward Responsibilities*** included in this document.)

4.1.1 Data Capture and Storage. Working with the Data Governance Council, an official data storage location, or system-of-record for each data element is identified by the Data Steward. An official data storage location for valid codes and values for each data element is identified by the appropriate Data Steward. University Enterprise Database data element definitions and codes are managed by the Data Steward to assure they are consistent across all applications, or that they conform to pre-established integration standards for code mappings and crosswalks between systems. Archiving requirements and strategies for storing and preserving archived historical data are pre-determined by the Data Steward for each University Enterprise Database data element. Information Technology assists in determining archiving requirements and data storage location for University Enterprise Database data.

4.1.2 Data Quality, Validation and Correction. Data Stewards are responsible for assuring that applications that capture and update University Enterprise Database data incorporate edit and

validation checks to protect the quality of the data. Any Data User may question the accuracy of any data element. The Data User is responsible for helping to correct the problem by supplying as much detailed information as possible about the nature of the problem. Data Stewards are responsible for assuring data quality, responding to questions about the accuracy of data in a timely manner, and correcting inconsistencies if necessary and where appropriate. Upon written identification and notification of erroneous data, corrective measures are taken as soon as possible to:

1. Correct the cause of the erroneous data.
2. Correct the data in the official active storage location. Historical warehouse data will not be changed or corrected.
3. Notify users who have received or accessed erroneous data.

4.1.3 Data Collection and Maintenance. Data Stewards are responsible for complete, accurate, valid, and timely data collection. Operational responsibility for data collection and maintenance is typically assigned to the Data Experts.

Delegation and decentralization of data collection and maintenance responsibility is encouraged in order to ensure that electronic data are efficiently updated at or near the data source or creation point. Furthermore, data-handling steps that do not add value should be eliminated. Procedures may be added instead to provide new informational status reports to interested parties.

4.1.4 Data Extracts and Reporting. Data Stewards are responsible for specifying business rules regarding the manipulation, modification, or reporting of University Enterprise Database System data elements. Data Stewards are also responsible for establishing standard University Enterprise Database data transformations to create pertinent summary or derived data. Note that summary or derived data are considered part of the University Enterprise Database and therefore subject to the same data management standards. If an element is derived the associated elements that were a factor in the derivation must be included in the University Enterprise database system and the derivation rules must be documented. All derived elements must be in tables or mapped via tables, report programs must not contain derivation logic.

Data Stewards are responsible for specifying proper dissemination of University Enterprise Database data; individual Data Users are held accountable for their own use of the data for internal reporting (see *Other Related WPU Tech Policies* www.wpunj.edu/it/policies).

All sets of data extracted or reported from the University Enterprise Database System should include a notation or display of the time and date they were extracted from the source operational system/s so the currency of disseminated data can be clearly communicated. Semester data must include the term as well.

Data Stewards work with Data Users to define useful and meaningful schedules for creating standard data extracts, including the census data extracts. These standard extracts of the data ("data snapshots") are considered part of the University Enterprise Database System and therefore subject to the same data management standards. The census data extract data will contain a census data element indicating the census term.

4.1.4.1 Data Views. A data view is a logical collection of data elements, assembled and presented according to a prescribed set of rules. Unlike a data extract that captures data at a fixed point-in-time and often includes moving the data to a secondary physical storage location, a data view is a logical subset of stored data. A data view typically assembles the most current or pertinent data from the primary storage location at the time of access. Data views are often defined in order to:

Supply data derived from standardized calculations or analysis,
Aggregate data from multiple sources,
Segment data into smaller and more manageable subsets, or
Segregate data according to confidentiality or restriction characteristics so that access to the resulting subset may be more widely distributed.

Data Stewards are responsible for defining standard data views of enterprise data within the University Enterprise Database. These data views are considered part of the University Enterprise Database and therefore subject to the same data management standards.

Data Experts, Data Managers, or Data Users may recommend the modification or definition of data views.

4.1.4.2 Data Archiving. Data Stewards are responsible for defining the criteria for archiving the data to satisfy data retention requirements. Data Managers work with Information Technology to develop appropriate data archiving strategies and procedures. Note that the capture of historical data into a Data Warehouse does not relieve the Data Steward of the responsibility for maintaining archives of detail transactional data in accordance with legal record retention requirements.

4.1.4.3 Data Warehousing. The Enterprise Information Systems (EIS) department, along with the Data Stewards, are jointly responsible for establishing an informational database known as the Data Warehouse. The Data Warehouse stores sharable historic data from operational systems-of-record, as well as transactional data derived from the operational data and deemed to be useful management information. It supports Data User queries to track and respond to business trends and to facilitate forecasting and planning efforts. Note that the Data Warehouse may contain summarized data derived from transaction detail and may not contain all the supporting transaction detail stored in the operational system-of-record or in the data archives.

The Data Warehouse design is based on a ***Data Integration Model,*** which is a logical construct that describes entities that comprise the University Enterprise Database System (UEDS). The Data Integration Model clarifies the linkages among data collected or maintained by the various organizational units of the university. The Data Stewards work with the Information Technology organization to develop and maintain the Data Integration Model. The Enterprise Information Systems (EIS) department provides expertise and software tools for data modeling.

A ***Metadata Repository***, which contains both technical and business descriptions and definitions about University Enterprise Database data, is a complementary facet of the Data Warehouse. It assists the Data User with understanding the source, meaning and proper use of the warehoused data. The Data Steward works with the Information Technology organization to develop and

maintain the Metadata Repository. Data Experts typically supply the business description metadata. The University uses datacookbook as the Metadata Repository.

4.1.5 Data Documentation. Documenting University Enterprise Database data is the responsibility of the Data Stewards. Some or all of the related tasks are assigned to Data Experts or Data Managers. Data documentation and definition guidelines are established by the Enterprise Information Systems department and include the following:

Name and Alias Names
Business Description
Data Steward Identification
Usage and Relationships
Source and Procedure for Data Capture
Frequency of Update
Official System-of-Record Location and Format
Designation as "Limited-access," "University-internal," or "Public"
For "Limited-access" Data Elements: Descriptions of the restriction and the access procedures
Description of Validation Criteria and/or Edit Checks Description, Meaning, and Location of Allowable Codes Archiving Requirements and Procedures
Data Storage Location of Extracts
Quality/Reliability Rating

Documentation for derived University Enterprise Database data should also include the algorithms or decision rules for the derivation. Documentation of data views should include reference to the data elements which comprise the view and description of the rules by which the view is constructed. If the derived element is warehoused and was derived from operational data the associated elements will be warehoused in the table with the derived element.

Overview documentation for logical segments of the University Enterprise Database (databases, files, groups of files) should also be provided to include information about data structure and update-cycles necessary for the accurate interpretation of the data.

Documentation of warehoused data are stored in the datacookbook metadata repository. The following guidelines are to be implemented concurrently with implementation of a Data Warehouse:

Information Warehousing Access specifies a standard data format for receiving and loading data definitions and descriptions into a Metadata Repository.

Data Stewards provide Information Warehousing Access with data definitions and other descriptive documentation in the prescribed standard machine-readable format.

Information Warehousing Access is responsible for the data administration function of maintaining a Metadata Repository for the Data Warehouse and for making it readily accessible to all interested parties.
Changes to any data definition characteristics should be noted to IWA and recorded in the Metadata Repository at the time of the change.

4.2 Access and Security Administration

4.2.1 Data Access Philosophy. The value of data as a university resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. Furthermore, increased data access and use improves data quality because discrepancies are identified and errors are subsequently corrected. As an educational institution with a mission to disseminate knowledge, and as a public institution accountable to the state of New Jersey, William Paterson University values ease of reporting information, including administrative data in a format appropriate for review. Permission to view or query data contained in the University Enterprise Database should be granted to all Data Users for all legitimate purposes. Update access should be restricted as necessary, but granted to university employees at the location where data are initially received or originates whenever this is feasible. Information specifically protected by law or regulation must be rigorously protected from inappropriate access. Examples include student grades, birthdates or personnel evaluations that are identifiable with a specific person.

4.2.2 Data Access Categories. As part of the data definition process, Data Stewards assign each data element and each data view in the University Enterprise Database to one of three data access categories:

University-internal
Public
Limited-access

*Except as noted below, all enterprise data are designated as **university-internal** data for use within the university.*

All university employees have access to these data, without restriction or prior authorization, for use in the conduct of university business. These data, while freely available within the university, are not designated as open to the general public.

Where appropriate, Data Stewards may identify elements or views of the University Enterprise Data Base that have no access restriction whatsoever. *Designated **Public** data may be released to the general public*.

Where necessary, Data Stewards may specify some data elements as limited-access. *Designated **Limited-access** data includes those data for which Data Users must obtain individual authorization prior to access, or to which only **need-based** access may be granted.*

When data are designated as Limited-access, the Data Steward should provide the following to the Information Technology Security and Data Base Administrators:

1. Specific reference to the legal, ethical, or externally imposed constraint which requires the restriction.
2. Description of Data User categories that are typically given access to the data, under what conditions, or with what limitations.

3. Documentation of the process for approving and implementing access.
4. Documentation of the process for maintaining security controls.

Note that a data view can possibly have more open access than that of the underlying data elements that comprise it. For example, removal of person-identifying data elements from a view may result in a view that contains some otherwise-restricted data elements but that the Data Steward may now designate as public or university-internal.

The appropriate Data Steward in collaboration with Information Resource Management is responsible for determining and documenting data access procedures that are unique to a specific information resource, view, or set of data elements.

Any Data User may request that a Data Steward review the restrictions placed on a data element or data view, or review a decision to deny access to Limited-access data. The appropriate Data Trustee makes the final determination about restrictions and access rights for enterprise data.

4.2.3 Implementation of Security Controls. The Information Technology (IT) Security and Data Base Administrators and the Data Stewards share security administration responsibilities (i.e., the functions of specifying, implementing, and managing system and data access control). To the extent possible, the Data Stewards work together and with IT to define a single set of university procedures for requesting and authorizing access to limited-access data elements in the University Enterprise Database. Data Stewards and IT are jointly responsible for documenting these access request and authorization procedures. Data Stewards, with the assistance of Information Technology, are responsible for monitoring and annually reviewing security implementation and authorized access.

All Data Users who are cleared for the limited-access category of University Enterprise Database data must acknowledge that they understand the level of access provided and accept responsibility to both protect their access privileges and to maintain the confidentiality of the data they access. Data Stewards are responsible for defining and implementing procedures to assure that data are backed up and recoverable in response to events that could compromise data quality. Information Technology or other university organizations may assist in this effort.

Data Stewards may delegate specific security administration activities to operational staff.

The University Information Technology Security Officer role is responsible for maintaining a plan for security policies and practices and for keeping abreast of security related issues internally within the university community and externally throughout the information technology marketplace.

4.3 System Administration. University enterprise data may be stored on a variety of computing hardware platforms, provided such platforms are fully integrated components of a managed ***University Information System*** under the control of, or approved by Information Technology. Whenever university enterprise data are stored on any component of a university information system, that system component must have a defined ***System Administration*** function with a designated system administrator whose responsibilities include:

Physical site security
Administration of security and authorization systems backup, recovery, and system restart procedures
Data archiving capacity planning
Performance monitoring

4.4 User Support and Responsibilities. Data Stewards are responsible for providing user support to assist Data Users with interpretation and use of UEDS data. Data Stewards are responsible for providing documentation of the information resource and also training and consulting services as needed. These responsibilities may be delegated to Data Experts and Data Managers.

The Enterprise Information Systems (EIS) department assists with training classes on the sub-set of data included in the Data Warehouse. EIS also provides training and consulting on the use of available query and reporting tools. Other university departments may also assist in this effort.

Data users are held accountable for their own use and interpretation of the data and may be required to attend or participate in training prior to being allowed to access data in the University Enterprise Database. Data Users are also responsible for reading and adhering to FERPA (www.wpunj.edu/centerss/ferpa/FamilyEducationalRightsandPrivacyAct.pdf)principles and guidelines and the Information Technology Appropriate Use Policy (www.wpunj.edu/it/policies).

5.0 List of Data Steward Responsibilities

Data Stewards are responsible for the following activities in their respective functional area/s. Data Stewards may delegate these activities to Data Experts, Data Managers, or others as deemed appropriate.

1. Establish procedures for defining and changing data elements within the operational systems.
2. Work with Information Technology and other Data Stewards to establish and maintain a university-wide Data Integration Model that describes the data entities of the University Enterprise Database and the relationships among these entities.
3. Identify an official data storage location for each University Enterprise Database data element and for valid codes.
4. Work with Information Technology to determine data retention requirements and archiving strategies for storing and preserving historical operational data.
5. Work with Information Technology to insure that data element definitions and codes are consistent across all applications or that they conform to pre-established integration standards for code mappings and crosswalks between systems.
6. Assure data quality, respond to questions about the accuracy of data, and correct inconsistencies.
7. Assure data collection is complete, accurate, valid, timely, and that data are maintained as close as is possible to the source or creation point of the data.
8. Set business rules regarding the manipulation, modification, or reporting of University Enterprise Database data elements and for creating derived elements.

9. Work with Information Technology to establish an informational database known as the Data Warehouse to store historical sharable data from the operational system-of-record.
10. Define standard views of enterprise data within the University Enterprise Database.
11. Work with Data Users to define useful and meaningful schedules for creating standard data extracts. Provide data descriptions and other documentation of warehoused data to Information Technology in a standard machine-readable format for inclusion in a Metadata Repository.
12. Specify the proper dissemination of University Enterprise Database data and security requirements by assigning each data element and each data view to one of the three access categories.
13. Work with Information Technology to define and document a single set of procedures for requesting and authorizing access to limited-access data elements.
14. Work with Information Technology to monitor and periodically review security implementation and authorized access.
15. Work with Information Technology and others to define and implement procedures that assure data are backed up and recoverable in response to events that compromise data quality.
16. Work with Information Technology to provide effective user support through documentation, training and consultation.

6.0 Other Related WPU Policies (if any)

All William Paterson University policies are found at www.wpunj.edu/policies

7.0 References

University of Virginia Polytechnic: http://www.policies.vt.edu/7100.pdf
University of Nevada, Las Vegas: http://ir.unlv.edu/DGCouncil/index.html
EDUCAUSE: http://www.educause.edu/library/data-governance?page=631&filters=sm_cck_field_super_facet%3A%22EDUCAUSE%20Library%20Items%22%20tid%3A33184
Data Governance: A Necessity in an Integrated Information World. Danette McGilvray
Information Management Magazine, December 2006

8.0 Approval and Revisions

Original 12/23/2013
Revised 2/7/2014
Revised 4/28/2014
Revised 12/22/2017

K/OPRE/DATAMANAGEMENT/FinalWPUDataGovernance
12/22/2017