DUQUESNE UNIVERSITY
Computing and Technology Services

Data Governance Service Requirements	Effective Date: 7/1/2018 Responsible Officer: Charles Bartel, Vice President for Information Technology and Chief Information Officer

1. **Purpose:**

The purpose of the Data Governance Service Requirement is to ensure that data is created, maintained, secured, monitored, audited and used in a manner that contributes value to Duquesne University. As it relates to this service requirement, Duquesne University's data and information is referenced within this service requirement as "institutional data". This service requirement defines the appropriate controls for protecting the confidentiality, integrity and availability of institutional data.

2. **Service Requirements:**

Duquesne University's institutional data, in all forms, is one of the University's most valuable assets and must be maintained and protected as such. It is critical to ensure that institutional data is accurate and trusted to support our University mission.

These Service Requirements are based on the following principles:

1. Duquesne University's institutional data is information that is prepared, managed, used, or retained by an organization or individual related to the activities or operations of the University. Duquesne University Intellectual Property is managed by TAP 40: Intellectual Property Policy.
2. Any technology environment that stores, processes or transmits Duquesne University's institutional data shall be secured in a manner that is reasonable and appropriate as defined in this policy based on the level of risk assigned to the data classification.
3. Institutional data protections and controls are the responsibility of the entire Duquesne University community. Individuals who are authorized to access institutional data shall adhere to these service requirements.
4. Institutional data use must follow and adhere to University policies and any applicable federal, state, or local laws.

Misuse of any aspect of institutional data may result in the loss of access, University disciplinary actions and/or legal prosecution under federal, state and local laws, where applicable. Duquesne University reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove or otherwise alter any data, file, or system resource which may undermine the authorized use of any of the technology environment or which is used in violation of these service requirements, University rules or policies. The unauthorized or improper use of Duquesne University's technology environment, including the failure to comply with these service requirements, constitutes a violation which may result in the loss of access, University disciplinary actions and/or legal prosecution under federal, state and local laws,

where applicable. Users are expected to adhere to T.A.P. 26 - Computing and Ethics Guidelines, which can be found at http://www.duq.edu/taps.

The University reserves the right to amend these service requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws.

Institutional Data Classification Summary			
Data Classification	**Institutional Risk**	**Description**	**Examples**
Level 1 - Restricted Data	High	Institutional data that could seriously or adversely impact Duquesne University and/or could have consequences on our responsibility for safety and education if accessed by unauthorized individuals. Institutional data is considered as high risk related to compliance, reputation, and/or confidentiality/privacy concerns. This data should have the highest level of security controls applied.	- PII (Social Security Number-SSN, Driver's License Number) - Bank/Financial Account Information - Credit Card Information (PCI) - Student Protected Data (FERPA) - Gramm-Leach-Bliley Act (GLBA) - Health Protected Data (HIPAA) - General Data Protection Regulation (GDPR) - Human Resource Data - University Financial Data - Central Authentication Data
Level 2 - Internal Data	Medium	Institutional data that should be protected from general access and/or restricted to protected groups or individuals. A reasonable level of security controls should be applied.	- Non-Banner Information stored in and/or accessed via DORI - Institutional data not publicly available and not classified as restricted. - Intellectual Property Data
Level 3 - Public Data	None	All public institutional data. While little or no controls are required to protect this data, some levels of controls should be applied to prevent the unauthorized modification or destruction of the data.	- Generally accessible institutional data such as information accessible at www.duq.edu that does not require authentication to access.

Institutional Data Classification Service Requirements

Level 1 – Restricted Data:

Restricted data, in electronic format, shall only be accessed for essential business purposes. All controls must be appropriately designed to allow for authorized use only. In most cases, this data has been deemed essential for business operations and/or law requires the protection of this data, including compliance related areas that may include but is not limited to Family Educational Rights & Privacy Act (FERPA), Health Insurance Portability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), the EU General Data Protection Regulation (GDPR), Payment Card Industry (PCI), ACT 101 or Title IX.

- Storage. Restricted data in electronic format must be stored in an approved university data center and/or an approved institutional data repository. Restricted data can be stored on approved University file storage locations that provide appropriate data security controls including encryption, authentication, and authorization. Restricted data should not be stored in electronic format on University-owned owned computers/devices such as desktops, laptops, tablets and phones. Restricted data cannot be stored in electronic format on personally owned computers/devices including desktops, laptops, tablets and phones.
- Transmission. Restricted data in electronic format must be encrypted while in transit over a public network and the Duquesne University network (wired/wireless/VPN). Any transmission to a third party outside of the Duquesne University wired network must be encrypted.
- Authentication. Restricted data in electronic format must be protected and accessed by University secure authentication methods approved by CTS.
- Third party use. Restricted data in electronic format can be stored by University approved third parties. In order to be an approved third party the following conditions must be met.
    - A mutual non-disclosure agreement, agreed to by the third party and Duquesne University, must be executed.
    - The third party agrees to provide an appropriate SOC (Service Organization Control) report and that report is reviewed and approved by Computing and Technology Services (CTS).
    - A University contract reviewed and approved by Computing and Technology Services (CTS) and Legal Affairs, and executed by the Vice President for Finance and Business.

Level 2 – Internal Data:

Internal Data in electronic format, shall only be accessed for business purposes. Controls shall be appropriately designed to allow for authorized use only. Protection of this data is the responsibility of the University department that utilizes the data as a course of business. This data should not be related to any compliance related areas including but not limited to HIPAA, FERA, PCI, GLBA, ACT 101 or Title IX.

- Storage. Internal Data in electronic format can be stored on systems and applications residing in an approved University data center and/or an approved institutional data repository. Internal Data can be stored in electronic format on University-owned computers including desktops, laptops, and mobile devices. Internal data can be stored on University file storage locations that provide appropriate data security controls including authentication and authorization. While Internal Data isn't required to be encrypted, it is advised when possible.

- Transmission. Internal Data in electronic format must be encrypted while in transit over a public network. Internal Data is not required to be transmitted in an encrypted form while on the Duquesne University network (wired/wireless/VPN), but it is recommended to do so when possible. Any transmission of Internal Data off of the Duquesne University network to a third party is required to be encrypted.
- Authentication. Internal Data should be protected with secure authentication methods approved by CTS.
- Third party use. Internal Data transmitted to third parties or via the Duquesne University wireless network must be encrypted when considered confidential or when the privacy is required.

Level 3 – Public Data:

Public Data in electronic format can reside in the public domain such as a public website and can be accessible to all students, faculty, and staff. Protections of this data are at the discretion of the responsible University department, however industry standard protections should be applied to protect any institutional data.

3. Enforcement:

The unauthorized or improper use of Duquesne University's technology environment, including the failure to comply with these service requirements, constitutes a violation which may result in the loss of access, University disciplinary actions and/or legal prosecution under federal, state and local laws, where applicable. Users are expected to adhere to T.A.P. 26 - Computing and Ethics Guidelines which can be found at http://www.duq.edu/taps.

The University reserves the right to amend these service requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws.

Appendix A - Predefined Types of Restricted Information

Computing and Technology Services has defined several types of “Restricted Data” based on state and federal regulatory requirements. This data could potentially trigger compliance or breach obligations if not protected and encrypted. They're defined as follows:

1. Authentication Verifier

An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some instances, an Authentication Verifier may be shared amongst a small group of individuals when approved by CTS. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to:

- Passwords
- Shared secrets
- Cryptographic private keys

2. Electronically Transmitted Protected Health Information ("ePHI")

ePHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component. ePHI is considered individually identifiable if it contains one or more of the following identifiers:

- Name
- Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code that could identify an individual

ePHI does not include education records or treatment records covered by the Family Educational Rights and Privacy Act (FERPA) or employment records held by the University in its role as an employer.

3. **Federal Tax Information ("FTI")**

FTI is defined as any return, return information or taxpayer return information that is entrusted to the University by the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.

4. **Payment Card Information**

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

5. **Personally Identifiable Education Records**

Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers:

- Name of the student
- Name of the student's parent(s) or other family member(s)
- Social security number
- Student identification number (D-Number)
- A list of personal characteristics that would make the student's identity easily traceable
- Any other information or identifier that would make the student's identity easily traceable

See Duquesne University's FERPA Policy (http://duq.edu/work-at-du/human-resources-home/taps---the-administrative-policies/28-family-educational-rights-and-privacy-act-(ferpa)) for more information.

6. **Personally Identifiable Information**

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

a) Government Identification number

- Social security number – SSN (including last 4 digits of SSN)
- State-issued driver's license number
- State-issued identification card number

- Tribal identification number
- Passport number
- Alien registration number
- Voter identification number

b) Financial Records

- Credit Card number
- Debit Card number
- Checking account number
- Savings account number
- Personal Tax information
- Unique electronic identifiers
- Routing codes
- Passwords, personal identification numbers (PIN), or other access codes for financial or credit accounts
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account

c) Personal Identifiers (Can be used in combination with other attributes to create PII or threat to PII)

- Date of birth
- Mother's Maiden Name
- UserID and Password
- Parent's legal surname prior to marriage if this information would permit access to a person's financial account or resources
- Digital or electronic signatures

Revision Date	Reason for Change	Author
11/21/2017	Improvements to document.	Tom Dugas, Director of Information Security/New Initiatives
7/1/2018	Updates to reflect compliance regulations.	Tom Dugas, Chief Information Security Officer (CISO)Security/New Initiatives