Information/Data Access and Security Guiding Principles

October 30, 2015

Information/Data Access and Security

D3M Data Security and Access Objective:

Deliver the *right* information …

… to the *right* people …

… at the *right* time …

… to support the *right* decision.

Information/Data Access and Security
Guiding Principles

We recognize the importance of data in making effective and timely decisions. We therefore seek to make data available as easily and widely as possible while at the same time recognizing the importance of protecting highly sensitive or personal data. To achieve this, we will:

- Presume trust of those authorized with access to a set of data (i.e., faculty, staff, student, space)
- Not restrict access due to concern of misinterpretation or discovery of inaccurate or incomplete data
- Impose tight restrictions only when there is clear risk of significant harm to the University
- Require and periodically renew acknowledgment of and agreement with appropriate use policies
- Provide appropriate training and require, where applicable, certification
- Monitor and audit access to information in the Enterprise Data Warehouse to ensure continued compliance and effective stewardship
- Require that information gathered and analyzed for consumption by audiences outside of the University be vetted with appropriate stakeholders
- Ensure that the need for restricted-access, personally identifiable information associated with individual students is based on legitimate educational interest
- In general, make data that is available from other public sources accessible without restriction to all in the Notre Dame community

Information/Data Access and Security Establishment

To establish these Guiding Principles in practice, the offices of the President, Provost and Executive Vice President will:

- Support the role of the Information Governance Committee (for Highly Sensitive Information) and the Data Stewards (for all other information) to assign initial sensitivity and access designations to data elements

- Identify and designate certain information elements as restricted access. These elements include:
  a) Student grades, GPA, class rank, test scores, academic standing, disciplinary action, admissions status and financial aid information
  b) Faculty and staff compensation and performance evaluations
  c) Gender, Religion, Age, Ethnicity and Marital Status

- Review and vet access restrictions designated by the Information Governance Committee and Data Stewards. Assign the burden for justification of restricted access designation to the Data Steward making the designation.

- Charter the Campus Data Steward and the Information Governance Committee to draft and recommend an Appropriate Use Policy and a role-based access authorization process