INSTITUTIONAL DATA POLICY
Notes and Frequently Asked Questions (FAQ)

DRAFT -- 7 September 2010

1. Why do we need an Institutional Data Policy?

   The University community and external communities have expectations regarding the appropriate and ethical uses of data and their stewardship that are critical to MSU's ability to maintain public trust and confidence. These expectations are reflected in an expanding set of legally mandated protections for certain types of data, and in a similarly wide variety of protections that derive from institutional policies and contracts between MSU and third parties. It is important that everyone working with data at MSU be aware of specific legal, policy, and contractual requirements applicable to these data.

   Community norms also suggest that the University should have a single "umbrella" policy that provides an overall set of minimum expectations for the appropriate stewardship of data. This is the purpose of the Institutional Data Policy, which is also the appropriate home for the definition and examples of Confidential Data. Previously, these were a part of the Guidelines for Internal and External Reporting of Data System Security Breaches (http://lct.msu.edu/documents/SECURITY_BREACH_GUIDELINES_revised_Dec_2009.pdf).

2. Does this Policy override or obviate other, more specific policies or guidelines relating to Institutional Data, such as policies or guidelines that individual University units may have in place?

   No, it does not. MSU frequently is required by law, by industry practices, or by business contracts to protect certain types of data. Examples include personal health information under HIPAA, student education records under FERPA, and payment card data under Payment Card Industry Data Security Standards. MSU has policies and practices that reflect these obligations. These targeted policies and practices provide more specific guidance about handling these types of data. Similarly, University units that work actively with Confidential Data may find it useful to have unit-specific guidelines and work practices to help their employees understand the data protection expectations which they must meet. Unit-level guidelines should be consistent, overall, with this Policy.

3. Does this Policy address ownership of data held at MSU?

   This Policy does not address the ownership of Institutional Data or any other forms of content collected or created at MSU. This Policy sets minimum standards for responsible *use* of Institutional Data at MSU.

4. Does this Policy apply to volunteers and agents or contractors of MSU who might work with Institutional Data?

   Yes, indirectly. The Policy can only hold members of the University community -- faculty, staff and students -- directly responsible for compliance with the Policy. Section IV.C.4 of the Policy makes it clear, however, that those who are subject to this Policy need to take appropriate action to provide for the proper use, storage, and disposal of Institutional Data by others working with that Data under their supervision. This includes informing them of the Policy and any restrictions on the Data. In some circumstances, it may also include placing contractual restrictions on the further dissemination of the Data by those with whom the Data are shared.

5. Does the Policy apply to things like graphics, images, still photographs, movies and videos, animations and other non-text or non-numeric content?

   Yes, the use of the word "data" in the Policy is intended to include content in all forms and formats.

6. If a "data container" such as a report or record contains a mixture of Institutional Data that have been made Public Data, Institutional Data that have not been made Public Data, and/or Confidential Data, what rules apply to it?

   Whenever data types are mixed, the rules that apply are those applicable to the most restricted type of data in the mixture. For example, any combination of Institutional Data that contains Confidential Data must be treated as Confidential Data.

7. What is the geographic scope of this Policy? Does it apply to locations outside the main East Lansing, Michigan campus?

   The Policy applies to all MSU Institutional Data, no matter where they are or are used, from what location they may be accessed, or in what device they are held.

8. MSU is a public university. Doesn't this mean that all data at MSU are in the public domain?

No. The University is subject to a variety of legal and other obligations to restrict the disclosure of certain data and records. See Appendix I to the Policy. The University also is subject to various reporting and disclosure requirements relating to specific data and documents. Section V.A of the Policy makes clear that the Policy is not intended to impede the release of data or records when that is legally required. The existence of such requirements does not justify the lax or careless treatment of Institutional Data.

9. Does the Policy affect the sharing of Institutional Data among University offices?

No, provided that the Institutional Data is shared with members of the University community who have a University purpose for receiving it. Please note that members of the University community are expected to cooperate with the Freedom of Information Office in responding to Freedom of Information Act requests and with the Office of General Counsel and other University offices in complying with court orders, subpoenas, and other legal mandates for the release of Institutional Data.

10. Suppose an individual mistakenly believes Institutional Data have become Public Data and fails to take appropriate action to protect those Data. What will happen to that individual?

An individual who reasonably believes that certain data or records are Public Data (as defined by the Policy), and acts accordingly, should not be subjected to discipline under the Policy if it turns out that any such data or record is not, in fact, Public Data. The individual's belief must be objectively reasonable. If an individual is unsure whether any data or records are Public Data, he or she should check with the administrator of the unit from which he or she obtained access to that record or data.

11. How does the list of Confidential Data types and examples in this Policy and in Appendix I to this Policy relate to types and examples of confidential data that were previously part of the Guidelines for Internal and External Reporting of Data System Security Breaches ("Guidelines")?

This Policy is the appropriate "home" for these definitions and examples, and the Guidelines will be amended to cross-reference this Policy after its adoption.

12. To whom should suspected violations of this Policy be reported?

Employees (including student employees) may report suspected violations to their immediate supervisor or to the lead administrator of their employing unit.

Undergraduate students also may report suspected violations to the Office of the Associate Provost for Undergraduate Education and Dean of Undergraduate Studies; graduate students also may report suspected violations to the Office of the Associate Provost for Graduate Education and Dean of the Graduate School. Individuals may also report their concerns via the Fiscal Misconduct Hotline (http://ctlr.msu.edu/COMBP/FiscalMisconduct.aspx). Suspected violations of this Policy should be reported as soon as possible.

13. Regarding the training referred to in Section VI of the Policy, are there University resources available to help unit supervisors and administrators fulfill this responsibility?

    Unit supervisors and administrators should keep themselves and their staff informed about the types of Confidential Data with which their unit works. Together, they should make sure that their unit's handling of these Confidential Data comports with legal and policy requirements and best practices. General resources may be found in the Managing Sensitive Data portion of the Computing.msu.edu website (http://lct.msu.edu/guidelines-policies/#msd). Relevant University offices can assist with guidelines and training specific to particular Confidential Data types (see, for example, the offices listed in Policy Section VIII).

14. Does this policy keep me from using "cloud computing" services (i.e., services available on the Web)?

    Not necessarily -- it depends on the types of data involved and on the type of service being used and its terms of use. This Policy *does* require that each person using Institutional Data in cloud services take responsibility for appropriate use of those services. Guidance regarding use of cloud computing services may be found at http://lct.msu.edu/documents/LCT-Appropriate_Uses_of_Cloud_Computing_09_Nov_2009.pdf .