April 13, 2017

Office of General Counsel

Records Retention/Data Classifications/ Data Inventory

Daniel McCabe
Assistant General Counsel

Sarah McGee
Assistant General Counsel

PART ONE: RECORD RETENTION

STATE *of* MINNESOTA

Proclamation

WHEREAS: The authenticity of records and information is critical to protecting the rights and privacy of individuals, promoting compliance and profitability of business and organizations, and enabling governmental agencies to serve the best interest of those within their jurisdictions; and

WHEREAS: Records and information management professionals are responsible for the systematic control, maintenance, use, and disposition of the most important records of an organization, and play an important role in ensuring organizational effectiveness; and

WHEREAS: Control of records is necessary for the reduction of risk and liability associated with an organization's activities as well as for compliance with laws; and a successful records and information management program adheres to organization policies and procedures and incorporates sensible regulations to protect archival records for posterity; and

WHEREAS: Technology is increasing the amount of information gathered by organizations, and globalization is expanding the complexity of the information created, making proper management of information essential; and

WHEREAS: The Minnesota Government Records and Information Network (MN-GRIN) provides a forum for the exchange of knowledge among government individuals and agencies; and

WHEREAS: The Minnesota Department of Administration, Information Policy Analysis Division (IPAD), provides assistance, training, education, and advice on Minnesota's public access and privacy laws to the public and government; and

WHEREAS: The Minnesota Historical Society supports localities and state agencies with efficient and economical management of their records and assists with the transfer of permanent records to the State Archives of the Minnesota Historical Society.

NOW, THEREFORE, I, MARK DAYTON, Governor of Minnesota, do hereby proclaim the month of April 2017, as:

RECORDS AND INFORMATION MANAGEMENT MONTH

in the State of Minnesota.

IN WITNESS WHEREOF, I have hereunto set my hand and caused the Great Seal of the State of Minnesota to be affixed at the State Capitol this 31st day of March.

GOVERNOR

SECRETARY OF STATE

MINNESOTA STATE

RECORD RETENTION: INTRODUCTION

- Minn. Stat. § 15.17, Minn. Stat. § 138.17, Minn. Stat. § 138.19, and the Minnesota Government Data Practices Act set forth general record retention requirements for state agencies
- Records must be kept so that the public can have accurate knowledge of official activities, so that the campuses can conduct business, for legal purposes, and for historical purposes
- Likewise, records that no longer have value should be disposed of in accordance with a record retention schedule

RECORD RETENTION: WHAT NEEDS TO BE KEPT

- Records can have administrative value, legal value, financial value, or historical value
- Examples include correspondence, contracts, architectural plans, final budgets, financial statements, and official meeting minutes
- Notes and drafts are not official records

RECORD RETENTION: RETENTION POLICIES

- Record retention policies set forth how long the schools and colleges need to keep records
- Record retention schedules should keep in mind the value of records
- The policies have to be approved by the Minnesota Records Disposition Panel
- The Minnesota Historical Society has resources on its website to walk you through the process of getting a record retention policy approved

RECORD RETENTION: CREATING A SCHEDULE

- List the data you create and maintain
- See if data is covered by an existing schedule
- For example, the System follows the Minnesota State Personnel and Payroll Schedule for HR records

RECORD RETENTION: CREATING A SCHEDULE

- Consult with the Office of the General Counsel and other schools to find out what a retention schedule can include
- Consult with the Minnesota Historical Society
  - www.mnhs.org/preserve/records

RECORD RETENTION: GETTING APPROVAL

- The Minnesota Historical Society can assist with getting approval of your record retention schedule

- www.mnhs.org/preserve/records/recser.php

RECORD RETENTION: FOLLOWING THE SCHEDULE

- Provide appropriate notice to the Minnesota Historical Society when records are destroyed
- Don’t keep records longer than the schedule sets forth unless necessary
- Update the schedule as needed

RECORD RETENTION & THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

- Records must be maintained so that they are easily accessible in the event of a data practices request
- Tips for record maintenance include keeping well organized electronic files, using shared drives, and keeping well documented keys and catalogues of hard files

PART TWO: DATA CLASSIFICATION

New Procedures

- System Procedure 5.32.2 Data Security Classification
  - Operating Instruction 5.23.2.1 Data Security Classification (formerly “Guidelines”)
- System Procedure 5.23.3 Information Security Requirements and Controls
  - Operating Instruction 5.23.2.2 Information Security Controls

Data Classification

- The process of organizing our data categories to apply appropriate security controls to protect the security and confidentiality of not public data.
- Why?
  - Good practice
  - Minn. Stat. § 13.05, subd 5 requires state agencies to establish "procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure;"
- The System Procedures and Operating Guidelines apply to all government data.
  - Not just official records
  - Not just electronic data

5.23.2 Data Security Classification

- **Data owner**: the individual with the authority and accountability for specified information.
  - Designated by the Chancellor and presidents for all departments
  - Usually a person in a senior or leadership position
  - May be more than one at a College/University
- **Data custodian**: appointed by the data owner to assign the classification and ensure appropriate controls.
  - Must document the classification of all data
  - Must re-review classifications every 3 years

5.23.2 Data Security Classification cont'd

- All data must be classified in one of three security classifications:
  - Highly Restricted
  - Restricted
  - Low
- Data owner must also maintain a data inventory that complies with Minn. Stat. § 13.025, subd. 1

5.23.2.1 Data Security Classification Operating Instructions

- Highly Restricted Data
  - SSNs
  - Credit Card or other payment card numbers
  - Financial account numbers
  - Security or access codes and passwords
  - Personal health information
  - Non-public investigation data
  - IT Credentials for systems that manage restricted data
  - Biometric data
  - Trade secret data or other intellectual property protected by a non-disclosure agreement

5.23.2.1 Data Security Classification Operating Instructions cont'd

- Low
  - All public data. Includes directory data for students and certain personnel data.
  - Anything available in response to a MGDPA request
- Restricted Data
  - Is not public by law and
  - Is not one of the categories listed as "Highly Restricted."
    - Class lists, grades, other student records (including directory information if suppressed)
    - Most personnel data
    - Donor contact information
    - ID numbers if not directory data
    - RFP data prior to contract award
    - Business continuity plans
    - Other security data

5.23.2.1 Data Security Classification Operating Instructions cont'd

- What if I can't tell?
  - Vice Chancellor for Information Technology
    - Potential negative financial impact or identity theft
    - Potential legal/regulatory action
    - Reputational damage
    - Other violation of law
- What if a collection has different types?
  - You can classify the entire collection at the most restrictive level.

5.23.2.1 Data Security Classification Operating Instructions cont'd

- When?
  - Identify data owners and custodians by June 8, 2017
  - Inventory IT systems containing data by December 8, 2017
  - All highly restricted elements classified by March 8, 2018
  - All other data elements classified by September 8, 2018.

5.23.3 Information Security Requirements and Controls

- Once you've classified the data as Highly Restricted, Restricted, or Low, the appropriate controls have to be placed to the data to secure access.
- What's an information security requirement?
  - Information security obligations that must be met or implemented. Information security requirements are defined by, for example, federal or state law or regulation, industry regulations, state statute, board policy or procedures, third-party contracts, college or university policy, or any other information security protection requirement identified by the data owner.
  - It's the "WHAT"
- What's an information security control?
  - Technical, administrative, management, or physical methods or safeguards that, when applied satisfy information security requirements.
  - It's the "HOW"
- Example: an information security requirement may state, "confidential data in transit over a public network (i.e., Internet) must be unreadable to any unauthorized individual." The information security control for meeting this requirement could be to apply encryption to any confidential data when it is transmitted over the Internet.

5.23.3 Information Security Requirements and Controls cont'd

- Data owners must:
  - identify information security requirements applicable to any institutional data or IT system for which he or she is responsible and
  - ensure that any information technology service provider that provides an IT service meets applicable requirements.
- Data custodians must:
  - use the operating instructions to determine the appropriate security controls to meet the information security requirements for the IT systems and data for which they are responsible.
  - Use questionnaires and mapping tables in the operating instructions.
  - Apply answers to "assurance profiles" – a list of non-functional requirements for the protection of data confidentiality (C) and data integrity (I).

5.23.3.1

User Impact Mapping

Subpart B.1. User Impact Mapping Table

Impact Rating	User Impact: Low number of individuals' not public information (<250)	Medium number of individuals' not public information (250 – 24,999)	High number of individuals' not public information (25,000 – 249,999)	Very high number of individuals' not public information (>250,000)
Confidentiality:				
Highly restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Low**	**C-Medium**	**C-Medium**	**C-High**
Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Low**	**C-Medium**	**C-Medium**
Low data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Minimum**	**C-Minimum**	**C-Minimum**
Integrity:				
Data that affects the financial position of the organization or IT systems that contain official academic records	**I-Low**	**I-Medium**	**I-Medium**	**I-High**
Used to make financial, academic, or personnel decisions	**I-Low**	**I-Low**	**I-Low**	**I-Medium**
Informational only	**I-Minimum**	**I-Minimum**	**I-Minimum**	**I-Minimum**

Assurance Profiles

Subpart C. Data confidentiality medium (C-Medium)
Include all of *Data Confidentiality Minimum and Low,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum or low, or it may be a new requirement:

NFR – Security - configuration integrity

- **B1** - A non-refutable log of all access and modifications to the IT system configuration by accounts with privileges sufficient to modify IT system configuration will exist and contain action performed, individual, IP address, date and time for a period of one year
- **B2** - No more than one business day of IT system modifications will be lost
- **B3** - Access and modification of IT system configuration will be conducted using privileges limited to the minimum required to complete the activity

NFR – Security - configuration assessment

- **B1** - The configuration of the IT system will be verified by automated rule based systems at intervals no longer than 30 days
- **B2** - The configuration of the IT system will be compared against Center for Internet Security (CIS) level 1 or equivalent and differences documented
- **B3** - A formal process exists for assessing configuration modifications prior to implementation

NFR – Security - data access

- **B1** - The IT system will maintain a non-refutable log of all access and modifications to highly restricted IT system managed data sufficient to determine the individual, IP address, date, and time
- **B2** - Multi-factor authentication is required for each individual accessing or modifying the IT system configuration
- **B3** - Tools and processes exist that detect, log, and alert on unauthorized access to the IT system and to data managed by the IT system

WHEN?

- Required Date of Implementation
  - High Assurance Profile IT systems or services within eighteen (18) months from date of operating instructions adoption (September 2018)
  - Medium, Low and Minimum Assurance Profile IT systems or services Within twenty-four (24) months from date (March 2019)

PART THREE: DATA INVENTORY

DATA INVENTORIES: WHAT IS A DATA INVENTORY?

- The Minnesota Government Data Practices Act 13.025 requirement
- Document that provides contact information for “responsible authority” and describes categories of data on individuals maintained by the entity
- The “responsible authority” is typically the President of your college or university
- Data on individuals means data related to a specific person

DATA INVENTORIES: WHAT NEEDS TO BE IN DATA INVENTORY?

- Contact information for responsible authority (name, title, address)

- Description of each category of record, file, or process that you keep relating to data on individuals

DATA INVENTORIES: HOW TO PUT ONE TOGETHER

- There are data categories in the MGDPA
- Go through those categories, see what data sets your campus maintains
- Then, determine if the data you maintain is public, private, or confidential
- For ease of use of the inventory, the inventory can also cite the MGDPA provision regarding the data and who on campus has access

DATA INVENTORIES: MAKE AVAILABLE

- Data inventories must be available to the public
- The easiest way to do this is to publish it on your website
- The System Office recently completed its data inventory. It can be found at: http://www.minnstate.edu/system/ogc/dataprivacy/documents/minnesota-state-data-inventory-04.11.2017.pdf
- Admin has a data inventory located at: http://www.ipad.state.mn.us/docs/admin-inventory.pdf

Contact Information
Minnesota State Colleges & Universities
System Office

Daniel McCabe
Assistant General Counsel
Daniel.McCabe@minnstate.edu
651-201-1833

Sarah McGee
Assistant General Counsel
Sarah.McGee@minnstate.edu
651-201-1410

MINNESOTA STATE