Augsburg University

Electronic and physical data classification, protection, gathering, and reporting policy

I. Purpose

This policy defines Augsburg's data classification scheme and sets the minimum requirements for securing data in electronic or physical form that is collected, stored, processed, received, sent, or maintained by or on behalf of Augsburg. Data owned, used, created or maintained by Augsburg is classified into the following three categories:

1. Public
2. Regulated
3. Confidential

Departments should carefully evaluate the appropriate data classification category for their information. When provided in this policy, examples are illustrative only, and serve as identification of implementation practices rather than specific requirements.

II. Scope

This classification applies to all Augsburg data regardless of the storage medium (e.g., hard copy vs. digital/electronic).

III. Definitions

A. **Public**
Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. By way of illustration only, some examples of Public data include:
   1. Publicly posted press releases
   2. Publicly posted schedules of classes
   3. Publicly posted interactive maps, newsletters, newspapers and magazines
   4. Public announcements, advertisements, directory information, and other freely available data on Augsburg websites

B. **Regulated**
Regulated data is information that is protected or required to be collected and reported in aggregate form by statutes, regulations, institutional policies or contractual language. By way of illustration only, some examples of regulated data include:
   1. Student record information (i.e. protected by FERPA)
   2. Prospective students

3. Employee information
4. Financial records
5. Physical plant details
6. Credit card numbers (i.e. regulated by PCI-DSS)
7. Health records (i.e. regulated by HIPAA)

Regulated data:

1. Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure.
2. Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.
3. Must not be posted on any public website.
4. Must be destroyed when no longer needed subject to Augsburg's Records Retention Policy. Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal. Disposal of electronic equipment must be performed in accordance with Augsburg's standard practices of removal of data from electronic devices.

Personal Information Requiring Notification (PIRN):
PIRN is a subset of regulated data requiring special protection because its loss or theft *requires notification of the victims* by virtue of Minnesota Law.

In Minnesota, PIRN is defined as a person's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such a person:

- Social Security number
- Driver's license number or state-issued identification card number
- Financial account number, credit or debit card number, in combination with any required security code, access code, personal identification number or password, that would permit access to an individual's financial account
- Passport number

However, information is not PIRN if it includes data that is lawfully obtained from publicly available sources, or from federal, state or local government records lawfully made available to the general public.

C. **Confidential**

Confidential data is information that must be guarded due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Confidential data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data. By way of illustration only, some examples of Confidential data include:

1. Information maintained by the Office of the Provost
2. Alumni/Advancement information (unless permission for release is granted)
3. Donor/prospect information
4. Research data

5. Performance reviews
6. Donor profiles
7. Student data in the Center for Wellness and Counseling, Campus Ministry, or StepUP®

IV. Rules for managing regulated data

A. Collecting Regulated Data.

There are laws relating to institutional collection of regulated data based on the specific data. The legal restrictions most commonly impacting the institution are summarized below.

1. Regulated data may only be collected, maintained, used, or disseminated as necessary to accomplish a proper academic or business purpose of the university or as required by law.
2. Individuals or units requesting or collecting regulated data must communicate why the regulated data is being collected, how it will be used, and, if applicable, any consequences of not providing it.
3. Individuals may have the right to inspect and challenge, correct, or explain their personal information.

B. Sending and/or Receiving regulated Data in Electronic or Physical Form.

The following restrictions apply both to internal data transmissions (such as sharing files with another employee) as well as transmissions to outside parties.

1. Regulated data sent and/or received electronically must be secured using encryption technology, a secure web transfer, or the Secure File Transfer Protocol. Other acceptable methods include transferring files between network drives on the internal network. The institutional email system is not designed to support the transmission of regulated data securely. If email must be used to transmit regulated data individuals are instructed to contact their Liaison for Computing for guidance on securing the data.[1]
2. Routine exchange of regulated data with a third party requires a signed interoperability agreement or other contract describing which party is responsible for securing regulated data in transit and how the data will be secured, and any specific confidentiality obligations.
3. For any other release of regulated data by the institution to a third party the sender must ensure that the third party is aware of the confidentiality obligations applicable.
4. Regulated data sent in physical form, such as through the post office or interdepartmental mail, must be secured in a sealed envelope or similar method and marked confidential.
5. Faxing regulated data is permitted provided that the recipient is notified in advance and is available to retrieve the fax immediately following transmission or able to secure it upon receipt (i.e. receiving a fax in an office that is only accessible by the recipient). Individuals receiving faxed documents with regulated data are responsible for securing the document after receipt.

C. Storing regulated Data

1. Regulated data should be kept on IT administered servers. If regulated data must be stored on personal or university-owned devices, including but not limited to laptops,

[1] Emailing of grades is a generally accepted exception to this guideline if and only if both the faculty and student are using Augsburg email accounts. Using the learning management system (moodle) is preferred.

personal computers, CDs, flash or thumb drives, cell phones, and/or personal computing devices (i.e. smartphones, tablets, etc...), the regulated data must be encrypted (either stored on an encrypted hard drive or the data itself encrypted) and said devices must be password protected. All institutional laptops are encrypted automatically. Institutional desktops can be encrypted as needed.

2. Guidance on storage of regulated data can be found on the Regulated Data Storage Chart.
3. Regulated data saved in non-electronic form (i.e. paper or a whiteboard) must be protected from unauthorized access when left unattended and destroyed when it is no longer needed. For example, papers with regulated data cannot be left on an unattended desk but instead must be filed in a locked cabinet or a locked office.

V. Questions and Concerns

A. Questions about this policy can be directed to the Chief Information Officer.
B. If there is a concern that data may have been at risk of loss, theft, or unauthorized access one should contact their Liaison for Computing or the Chief Information Officer.

Revision History

Revision	Change	Date
1.0	Original Version.	10/13/2015
1.1	Added PIRN section.	12/18/2015
1.2	Added Questions and Concerns section. Small revisions elsewhere.	08/17/2016