Data Security Policy

A. Purpose and Overview

In the course of their employment, most law school employees will be exposed to data and information that is sensitive; confidential; proprietary to the law school or its partners or vendors; or subject to FERPA, HIPAA, privacy laws, or other laws restricting disclosure ("**Protected Information**"). Examples of Protected Information include, but are not limited to:

1. Student files and records (admissions files and data, academic records and grades, financial aid files and data, etc.);
2. Employee files and records;
3. Sensitive information related to students, employees, and others (Social Security numbers, credit card numbers, etc.);
4. Confidential information about JMLS and its business (financial and budget information, business plans, non-public reports and data, etc.);
5. Third-party information protected by confidentiality obligation or other prohibition on disclosure; and
6. Any extracts, spreadsheets, reports, and other compilations of information derived from the foregoing categories.

Each employee will take all necessary measures to protect and secure Protected Information from unauthorized access or disclosure. This policy governs the storage of Protected Information in electronic formats, and access and use of those electronic files.

B. Storing Protected Information

Employees must:

1. Store Protected Information in a JMLS-sanctioned, password-protected environment.
2. Store business-critical information in a location that is backed up by the JMLS ITS department or by a third-party vendor of JMLS.
3. Safeguard against the loss, theft, or misappropriation of removable media (flash drives, external hard drives, etc.) used to store Protected Information. In addition, employees must completely erase Protected Information from removable media before discarding or transferring the storage device.

C. Accessing Protected Information

Employees must:

1. Use passwords that are sufficiently "strong" and comply with password-strength requirements established by the JMLS ITS department.

2. Properly safeguard passwords and avoid insecure storage of passwords. Examples of insecure storage include:
    a. Keeping passwords in hard copy in an office or unlocked location;
    b. Storing passwords in an email folder or digital contacts list; and
    c. Storing passwords in a Word document or other electronic file saved to one's computer.
3. Not share individual passwords, even with co-workers.
4. Enable appropriate security mechanisms on smartphones, tablets, and other devices used to access JMLS email accounts or other sources of Protected Information.
5. Enable apps and services that allow a lost or stolen device to be locked or wiped clean of data.

D. Using and Disseminating Protected Information

Employees must:

1. Access, disseminate, or share Protected Information only as necessary for JMLS business purposes and only with persons who have a legitimate need to know such information to conduct JMLS business.
2. Delete or destroy unnecessary copies of Protected Information, unless notified of a litigation hold or other reason to preserve these copies.

E. Reporting Data Incidents

1. Employees must promptly notify JMLS of any actual, attempted, or suspected unauthorized access, use, disclosure, modification, or destruction of Protected Information (a "**Data Incident**"), so that JMLS may take all necessary and appropriate steps to investigate, contain, and remediate the potential or actual Data Incident and to comply with all applicable legal notice obligations and other legal requirements.

2. Notification must be to the JMLS ITS department at ITEmergency@jmls.edu, or (312) 427-2737, ext. 301. The individual leaving the notification should give his or her name and contact information, including email address and phone number. In addition, the individual should provide as much of the following information as possible:

    a. The date, time, and location of the Data Incident;
    b. A general description of the type of the Data Incident (e.g., hacking event, malware, lost laptop, etc.);
    c. The Protected Information or other confidential, nonpublic information and any computer system, application, or storage medium affected or at risk; and
    d. Any actions undertaken since discovering the Data Incident.

3. The individual reporting should also be prepared to assist the JMLS ITS department by providing any other details related to the Data Incident needed to assess, investigate, or remedy the situation.

F. Updating This Policy

This policy may be amended from time to time by the JMLS ITS department with the approval of the Dean.

Effective date: Administrative policy effective January 27, 2017.