Data Security Policy

Note: All community members should refer to Olin College's data classification policy for detailed information regarding the terms "Confidential data" and "Restricted data."

Guidelines for all community members:

1. No member of the Olin College community is permitted to electronically store or maintain **credit card or debit card numbers, expiration dates, and/or security codes** in any way relating to Olin or Olin-sponsored activities. IT must approve the use of any system or application that electronically processes, stores, or transmits credit card data.

   Paper documents containing credit card data should be secured in a locked office and stored in a cabinet. In an open office environment paper documents should be stored in locked cabinets. Paper documents should not be left in an unsecured office after work hours.

   All credit card processing (e.g., online, phone, mail, over-the-counter, card-swiping) must be reviewed and approved by the Assistant Vice President for Financial Affairs.

2. The following Confidential data types can only be electronically stored on an IT managed server and can only be accessed from an IT managed computer.
   - **Social Security number**
   - **Driver's license number**
   - **State/Federal ID card number**
   - **Passport number**
   - **Financial account numbers (checking, savings, brokerage, CD. . .)**

   In the event that an exception is necessary in order to carry out the business of the College, the user must get written approval from both his/her Vice President as well as the Information Security Officer.

3. It is recommended that all other confidential data and restricted data types be electronically stored or accessed from the one of the following list of devices, in order of preference: IT managed server, IT managed desktop computer, encrypted laptop, encrypted mobile storage device. Any encrypted device must be encrypted using a process documented and approved by Information Technology and the administrator of such system must report to the Information Security Officer on system security related matters.

   When handling physical documents containing any Confidential and/or Restricted data types, the documents must be in your possession at all times; otherwise they should be stored in a secure location (e.g. room, file cabinet, etc.) to which only specifically-approved individuals have access through lock and key (physical or electronic). When the information is no longer needed, the physical documents must be shredded using a College-approved device prior to being discarded; or destroyed by a College-approved facility. Please refer to Olin's Document Retention and Destruction policies for more details.

   Confidential data and restricted data should not be taken or stored off-campus unless the user is specifically authorized to do so by a Vice President and notification of the authorization is sent to the Information Security Officer.

4. The Information Technology Department reserves the right to electronically scan all Olin-owned resources and resources connected to the Olin network for confidential data and restricted data. In the event that confidential data or restricted data is found in unauthorized locations, the Information Security Officer will follow-up with the responsible Vice President to remedy the situation.

5. Confidential data cannot be transmitted through any electronic messaging (i.e. email, instant messaging, text messaging) even to other authorized users. Confidential data in a physical format cannot be transmitted through untracked delivery methods. Campus mail and regular postal services are not tracked delivery methods.

6. To help ensure the security of all Olin network accounts, all passwords must meet the following complexity and security requirements.
    - It must contain a minimum of 8 characters
    - It must contain at least one character from 3 or more of the following 4 categories:
        1. An uppercase letter (A – Z)
        2. A lowercase letter (a – z)
        3. A number (0 – 9)
        4. A non alpha special character (~ ! @ # $ % ^ & * _ - + = ` | \ ( ) { } [ ] : ; ** ' < > , . ? /)
    - It cannot contain your name or username
    - It cannot repeat any of your last 4 passwords
    - You must change it at least once every 180 days
    - Passwords must never be written down or shared with other users.
    - All users should also register their network account with Olin College's Password Management application located at the following URL: https://password.olin.edu

7. Users who are authorized to access or maintain confidential data or restricted data must ensure that it is protected to the extent required by Olin policy or law after they obtain it. All data users are expected to:
    - Access data only in their conduct of College business.
    - Request only the minimum confidential data or restricted data necessary to perform their College business.
    - Respect the confidentiality and privacy of individuals whose records they may access.
    - Observe any ethical restrictions that apply to data to which they have access.
    - Know and abide by applicable laws or policies with respect to access, use, or disclosure of data.

8. Compliance with these data protection policies is the responsibility of all members of the College community. Violations of these policies will be dealt with seriously and will include sanctions, up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to the data as well as College information technology resources during investigation of an alleged abuse. Violations may also be subject to prosecution by state and federal authorities. Suspected violations of Olin's data protection policies must be reported to the Information Security Officer.

Olin College

Guidelines for Supervisors, Data Managers and Data Custodians:

1. Olin College employees who have supervisory responsibilities and whose job responsibilities include the maintenance or use of Confidential data or Restricted data are responsible for ensuring compliance with Olin's data security policies as well as initiating corrective action if needed. In implementing these policies, each supervisory personnel is responsible for the following:

    - Communicating this policy to personnel under their supervision.
    - Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect all College data.
    - Ensuring that employees under their supervision are properly trained in data management procedures.
    - Submitting an annual report to the Information Security Officer outlining departmental security practices and training participation

2. Electronic access to confidential data should be granted by authenticating to a central IT resource. If it is not possible to use a central IT authentication method, the application conducting the authentication must operate under the same policies as the central IT resource (password and user lockout rules must apply and user accounts must be tied to a unique user).

3. Authorization for access to confidential data or restricted data shall be specified and approved by the respective Data Manager or Data Custodian, and must be made in conjunction with authorization or signed acknowledgement from the requestor, or other official authority.

4. When negotiating contracts with third party vendors, staff must consider whether such vendors require access to College databases or to other filing systems containing confidential information. Vendors should be contractually obligated to implement data protection and security measures that match the College's practices. If a vendor or consultant is to have access to Confidential data, the contract must be reviewed by the Information Security Officer to ensure the resulting contract has the following elements defined:
    - The contract must describe the purpose for access to the data.
    - Any Confidential data in transit electronically to the vendor must be encrypted.
    - Vendors /Consultants should be held accountable for the security and protection of any data that is in their possession.
    - Consultants must not disclose, allow access to, or permit other use of data beyond what is outlined within the contract.
    - Method of access to the data must be defined.

    No consultant or contractor is permitted to store Social Security number, driver's License number, credit or debit card number, state/federal ID card numbers, passport numbers, or financial account numbers (checking, savings, brokerage, CD. . .) in any way relating to Olin or Olin-sponsored activities without the express written permission of the Information Security Officer.