Olin College of Engineering
Information Security Plan

Updated and Effective April 24, 2019

Introduction

In support of its educational mission, Olin College acquires, develops, maintains, and archives information. College information is found throughout the campus community in various forms as transmitted by print, electronically, and orally. Handling information in a legal, judicious, and secure way depends on employees making good decisions as they follow College policies. Those policies are intended to be in line with current laws and regulations and with concern for students, employees, and alumni and friends of Olin College.

Scope

In compliance with applicable Gramm Leach Bliley Act ("GLBA") Safeguards Rules as published by the Federal Trade Commission, this plan applies to the administrative, technical and physical security of all College data that is acquired, transmitted, processed, stored, transferred and/or maintained by Olin College or any Olin College auxiliary organization. It applies to all Olin students, employees, consultants, contractors or any person having access to College data in any form or format.

Purpose

The purpose of the Information Security Plan is to:

- Establish a College-wide approach to ensure the security and protection of College data in the College's custody, regardless of format.
- Prevent and protect against any anticipated threats and hazards to the security or integrity of College data.
- Prevent and protect against the unauthorized access to or use of College data, including confidential and personally identifiable information.
- Ensure College-wide compliance to applicable data and student record protection laws, regulations, policies and practices.
- Develop greater security awareness by educating the Olin community of each person's data security responsibilities.
- Establish processes for monitoring and reviewing the program.
- Establish procedures for responding to potential College data security incidents.

Policy

It is the policy of Olin College to maintain a comprehensive Information Security Program ("ISP") in compliance with the Gramm Leach Bliley Act ("GLBA") Safeguards Rule pursuant to 16 CFR 314. The objective of the College's ISP is to:

1. Ensure the security and confidentiality of College data in compliance with applicable GLBA rules as published by the Federal Trade Commission;

2. Protect against anticipated threats or hazards to the security or integrity of College data; and

3. Protect against unauthorized access to or use of College data that could result in substantial harm or inconvenience to any Olin customer.

The College's ISP incorporates, by reference, College-wide information security-related policies and associated controls that address the security and confidentiality of College Data.

Procedures

In compliance with the GLBA, the College's ISP includes the following elements:

1. Designation of an Information Security Task Force and ISP Coordinator;

2. Assessment of reasonably foreseeable risks, both internal and external;

3. Identification of safeguards for managing known risks with routine monitoring and testing of safeguards;

4. Oversight of contractual agreements with college service providers to ensure service providers are capable of safeguarding financial information; and

5. Evaluation, documentation, and adjustment to the ISP on an annual basis.

Information Security Task Force

The Information Security Task Force will

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
- Design and implement plans that put safeguards in place to minimize those risks, consistent with the requirements of applicable legislation including 201 CMR 17.00 (Standards for The Protection of Personal Information of Residents of the Commonwealth), GLBA (Gramm-Leach-Bliley Act), and other applicable laws and regulations; and
- Regularly monitor the effectiveness of those safeguards.

Information Security Officer

The Information Security Officer (ISO) has been designated as the College ISP Coordinator. In this role, the ISO is the College official who has oversight responsibility for the College's ISP as well as compliance with relevant regulations, policies, standards and guidelines. Specifically, the Information Security Officer or designee is responsible for the following:

- Review Olin data security policies to ensure alignment with current practices and regulatory requirements.
- Oversee data security policies and their enforcement.
- Oversee risk assessments and document identified risks to data.
- Works with Regulation Monitors and Data Managers to ensure all third-party vendors with access to Olin data are compliant.
- Oversee reported policy violations and data security investigations; report suspected data incidents; report any violations to the Office of Consumer Affairs and Business Regulation and to the Attorney General of the Commonwealth of Massachusetts.
- Serve as the point person(s) for all external inquiries involving data security compliance issues.
- Annually review Olin's Information Security program, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing confidential information.
- The current Information Security Officer is Manuel Amaral, Director of Information Technology Operations.

Regulation Monitors

College officials who have oversight responsibility for one or more regulations are referred to as Regulation Monitors. Regulation Monitors stay abreast of updates to their respective regulations, ensure policies are up to date and notify the Information Security Officer and Data Managers about changes. Regulation Monitors are as follows:

- FERPA – Associate Dean for Academic Programs and Registrar
- USA Patriot Act (as it relates to FERPA) – Associate Dean for Academic Programs and Registrar
- PCI DSS & PCA/DSS – Assistant VP of Financial Affairs, Chief Information Officer, Director of Information Technology Operations
- GLBA – Assistant VP of Financial Affairs, Director of Financial Aid
- HIPAA – Director of Human Resources
- Federal Rules of Civil Procedure (specifically e-Discovery) – Director of Human Resources
- Red Flags Rule – Assistant VP of Financial Affairs
- Massachusetts' Standards for the Protection of Personal Information – Chief Information Officer, Director of Information Technology Operations
- Mass Crime Law – Chief Information Officer, Director of Information Technology Operations
- Computer Fraud and Abuse Act – Chief Information Officer, Director of Information Technology Operations

- Sarbanes-Oxley – Assistant VP of Financial Affairs
- Personal Data Privacy and Security Act – Compliance Team
- Identity Theft Protection Act – Compliance Team
- EU General Data Protection Regulation (GDPR) – Chief Information Officer, Director of Information Technology Operations
- Other applicable laws and regulations – Compliance Team

Data Managers

College officials who have planning and policy-level responsibilities for data in their functional areas are considered Data Managers. The Data Managers are responsible for recommending policies, establishing procedures and guidelines for College-wide data administration activities, and training of Data Users on the proper handling of data. Data Managers, as individuals, have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data. In collaboration with the CIO and ISO, Data Managers are responsible for developing and applying standards for the management of institutional data, and for ensuring that Data Users are appropriately informed of security obligations associated with their data access. Lastly, Data Managers are responsible for collaborating with the CIO and ISO to evaluate the ability of service providers to comply with applicable regulations in the handling of personal information for which the College is responsible, and to ensure there are included in College contracts with those services providers provisions obligating them to comply in providing the contracted for services, and to obtain from such service providers written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of applicable laws and regulations. For historical reasons – because data and the responsibility for data have traditionally been organized along functional or subject-area boundaries – the Data Managers are established according to this same subject-area organizing principle. Current Data Managers are:

- Financial Data: Assistant VP for Financial Affairs
- Financial Aid Data: Director of Financial Aid
- Academic Data: Associate Dean for Academic Programs and Registrar
- System/Log Data: Director of Information Technology Operations
- Institutional Research and Assessment Data: Director of Institutional Research & Decision Support
- Constituent Data
    - Prospective Students: Assistant Director for Admission Systems and Operations
    - International Students: Primary Designated School Official (PDSO), currently the Associate Dean of Student Affairs
    - Student: Associate Dean for Academic Programs and Registrar
    - Veterans and Dependents of Veterans: Financial Operations Manager, Associate Dean for Academic Programs and Registrar
    - Faculty/Staff: Director of Human Resources and Director of Academic Affairs & Sponsored Programs
    - Alumni/Donor: Director of Advancement Services

Internal Risk Safeguards

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory.

- The amount of personal information collected must be limited to that amount reasonably necessary to accomplish legitimate business purposes, or necessary to comply with other state or federal regulations.
- Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish their legitimate business purpose or to enable the College to comply with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
- All security measures shall be reviewed at least annually, or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information. The Information Security Officer shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
- Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
- A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the College's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.
- Current employees' user-ID's and passwords must be changed periodically.
- Access to personal information shall be restricted to active users and active user accounts only.
- Employees are expected to report any suspicious or unauthorized use of customer information.
- Whenever there is an incident that requires notification under M.G.L. c. 93H, §3 (The General Laws of Massachusetts - Security Breaches) or other applicable law or regulation, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
- Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.

- At the end of the workday, all files and other records containing personal information must be secured in a manner that is consistent with the ISP's rules for protecting the security of personal information and those detailed policies provided.
- Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers. These departmental policies cannot remove or negate policies set forth by College policies.
- Access to electronically stored personal information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
- Visitors' access to protected data must be restricted. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with M.G.L. c. 93I (The General Laws of Massachusetts - Standards for Dispositions and Destruction of Records).

External Risk Safeguards

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory:

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing and/or storing personal information.
- There must be reasonably up-to-date versions of system security agent software; which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing and/or storing personal information in accordance with policies and procedures.
- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
- All computer systems must be monitored for unauthorized use of or access to personal information.

- There must be secure user authentication protocols in place, including:
    - Protocols for control of user IDs and other identifiers;
    - A reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
    - Control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
    - Restriction of access to active users and active user accounts only; and
    - Blocking of access to user identification after multiple unsuccessful attempts to gain access.
    - The secure access control measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to personal information.

Incident Response Protocol

In the event of a possible or suspected information security incident, the Information Security Officer (ISO) and CIO shall be notified immediately. The College retains the services of an external agent with expertise in information security incident response, policy, investigative forensics, and notification protocol. The ISO and/or CIO will coordinate notification to and activation of the external agent, and will notify the Assistant VP for Financial Affairs, who acts as the College's Risk Manager. If necessary, the ISO and/or CIO will activate the College's Crisis Response Team (CRT). Depending on the nature of the incident, the College will take appropriate remedial action in coordination with its retained external agent.