Massachusetts School of Law

Financial Information Security Plan

09/2023

Massachusetts School of Law Financial Information Security Plan

Purpose:

In accordance with The Financial Services Modernization Act of 1999, also known as the Gramm-Leach Bliley Act, and to protect the financial information of our students, faculty, and staff, MSL has adopted this Financial Information Security Plan. The goal of this document is to outline the measures we will take to comply with this Act, and to ensure an ongoing review mechanism to address requests to meet future privacy needs. Assistant Dean Sullivan shall serve as the Coordinator of the Plan, with the Director of Technology, Mick Coyne and the Director of Library and Information Services, Daniel Harayda, as well as other School Officers as needed.

Objectives :

We will strive to ensure the security and confidentiality of all students and other customers 'financial records and information. This information will be safeguarded to protect to the extent possible any unauthorized access to, or use of, such records in a manner which could cause substantial harm or inconvenience to any customer. We will also protect against any anticipated threats to the security or integrity of this financial information.

Risk Assessment: MSL will assess the risk to customer financial information from each of the following:

- Unauthorized access to data through software applications
- Unauthorized use of other users' accounts and passwords
- Unauthorized viewing of printed data or computer displayed financial data.
- Improper storage of printed financial data
- Unprotected documentation usable by intruders to access data.
- Improper destruction of printed financial material

Specific Information Security Plans:

- No financial information will be collected by any Department of the school, which is not necessary for the effective functioning of that Department.
- Printed copies of customer financial information will be disposed of using "Shred It", MSL account #13795384, MSL's third party shredding company which shreds onsite.
- All offices and storage rooms will be locked, and filing cabinets will be locked nightly.
- Printed copies of customer financial information are not to be left on desks at night in unlocked areas.
- Key control of all locked areas will be maintained by the main office staff and all user departments. All locks are replaced in the event of personnel changes.
- Computer workstations used to display customer financial information are not to be left unattended with that information displayed. Users of such information are to log off when they are away from their workstation for any significant period.
- Passwords are to be utilized, and kept confidential, at all times. Authenticating key fobs are to be stored in a secure area.
- MSL has determined the use of Social Security numbers as student identifiers is not safe and has moved to protect its student's financial information by using a random assigned identifier. Social Security numbers are still used for reporting to the IRS on 1098T forms and in processing requests for Financial Aid.
- All staff utilizing customer financial information (both existing and new hires) will be given a copy of this plan and asked to signify their acceptance of it provisions.
- All service providers to MSL with access to student financial information will be expected to implement and maintain safeguards for their data storage.
- MSL will remain in full compliance with the Family Educational Rights and Privacy Act.
- MSL will continually evaluate and, where necessary, amend this Plan to ensure that student financial information is protected. This testing will include regular evaluation of the effectiveness of the safeguards put into place, and the key controls, systems, and procedures.

The Gramm-Leach Bliley Act (GLBA) Information Security Plan

Purpose: The Gramm-Leach Bliley Act, also known as the Financial Modernization Act of 1999, establishes the minimum standards to protect all consumers' personal financial information. This Act includes the Financial Privacy Rule which governs the collection and disclosure of customer's personal financial information by financial institutions and the Safeguard Rule which requires all financial institutions to design, implement and maintain safeguards to protect customer information.

Reason for Policy: To ensure the security and confidentiality of private information and data, and to comply with GLBA, MSL adopted this Information Security Program for certain highly critical and private financial and related information. This security program applies to customer financial information ("covered data") MSL receives in the course of business as required by GLBA, as well as other confidential financial information the University has voluntarily chosen as a matter of policy to include within its scope. This document describes many of the activities MSL has established to maintain covered data according to legal and MSL requirements. This Information Security Program document is designed to provide an outline of the safeguards that apply to this information.

Entities Affected by this Policy: Any office or department on campus that either collects, maintains, or has access to records containing protected personal (non-public) financial information for students, faculty, or staff, including but not limited to:

- Admissions Office
- Business and Financial Aid Services
- Registrar
- Payroll
- Data Systems
- Student Accounts Office
- Career Services

The following is a list of third-party servicers who may maintain records with protected personal (non-public) financial information for students, faculty, or staff:

- ADP
- Inceptia – a school default management program.
- FAS – MSL third party servicer

Who Should Read this Policy: All persons who have access to the protected data, including Administration, Faculty and every employee that accesses handle or maintains MSL's records (electronic, paper, or other form) containing non-public financial information about a constituent who has a relationship with MSL. MSL's employees include full-, part-time and hourly staff members as well as student workers who access, handle, or maintain records, particularly in the Business & Financial Aid Services, Career Services (including fundraising and alumni affairs offices), and Admissions.

Employees who contract with service providers (third party vendors) who, in the ordinary course of MSL's business, are provided access to covered data. Service providers may include, but are not limited to, banks and financial institutions, businesses retained to transport and dispose of covered data, data analysis firms.

Overview: Many financial institutions collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories and social security numbers. GLBA requires financial institutions, which includes colleges and universities, to ensure the security and confidentiality of this type of information, whether it is paper, electronic or some other type of format. The GLBA also requires the school to develop, implement and maintain a comprehensive Information Security Program containing the administrative, technical, and physical safeguards that are appropriate based upon the school's size, complexity, and the nature of its activities. This Information Security Program has five components:

- Designating an employee or office responsible for coordinating the program.
- Conducting risk assessments to identify reasonably foreseeable security and privacy risks.

- Ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored.
- Overseeing service providers.
- Maintaining and adjusting this Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

Definitions:

- A Financial Institution is a company that offers financial products or services to individuals, like loans, financial or investment advice or insurance.
- A Customer is a consumer who has developed an ongoing relationship with a financial institution. In general, if the relationship between the financial institution and the individual is significant or long- term, the individual is a customer of the financial institution.
- A Consumer is an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family or household purposes, and means the legal representative of such an individual.
- Covered Data includes information obtained from a constituent with whom the school has a relationship while offering a financial product or service or conducting fundraising activities; or such information provided to the University from another institution. Constituents include students, employees, service providers, alumni, parents, and friends (friends are defined as prospective donors or volunteers who do not have other relationships to the University).
- A Financial Product or Service includes offering student loans, receiving income tax information from a current or prospective student's parents as a part of a financial aid application, offering credit or interest-bearing loans, and other miscellaneous financial services Examples of financial information relating to such products or services include bank account numbers, credit card numbers, income and credit histories, social security numbers and wills and other testamentary documents.
- Service Providers refer to all third parties who, in the ordinary course of the school's business, are provided access to covered data. Service providers may include businesses retained to transport and dispose of covered data and loan servicers.

Procedures:

Risk Assessment: The Information Security Program will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. Risk assessments will include consideration of risks in each area that has access to covered information. Risk assessments will include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures.

The Coordinator will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks, as well as risks unique to each area with covered data. The Coordinator will ensure that risk assessments are conducted at least annually and more frequently where required. The Coordinator will work with all responsible parties from MSL's Information Technology Department to conduct the system-wide risk assessment. The Coordinator may identify a responsible party in each unit with access to covered data to conduct the risk assessment, or employ other reasonable means to identify risks to the security, confidentiality and integrity of covered data in each area of the University with covered data.

Information Safeguards and Monitoring: The Information Security Program will verify that information safeguards are designed and implemented to control the risks identified in a risk assessment. The Coordinator will work with departments to ensure that reasonable safeguards and monitoring are implemented and cover each unit that has access to covered data. Such safeguards and monitoring will include the following:

Employee Management and Training: Safeguards for security will include management and training of those individuals with authorized access to covered data. The Coordinator will, working with other department heads, help to identify categories of employees or others who have access to covered data. The responsibility for employee training will reside with various individuals as deemed appropriate by the policy coordinator and the Information Security Officer.

Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing limitations to access and maintaining appropriate screening programs to detect computer hackers and viruses and implementing security patches.

Safeguards for information processing, storage, transmission, retrieval, and disposal may include:

- Requiring that financial information be collected only by departments which is necessary for the effective functioning of that department.
- Requiring electronic covered data be entered into a secure, password-protected system.
- Using secure connections to transmit data outside MSL.
- Using secure servers.
- Ensuring covered data is not stored on transportable media (zip drives, etc.).
- Permanently erase covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media before re-selling, transferring, recycling, or disposing of them.
- Storing physical records in secure LOCKED areas and limiting access to that area.
- Disposing of outdated records in the locked shredding bins to be shredded; ensuring third-party providers provide certification of secure method of shredding and/or disposal.
- Requiring that printed financial information be kept in locked offices and storage areas.
- Ensuring that computer workstations used to access financial information are not left unattended with that information displayed. Users of such information are required to log off when they are away from their workstation.
- Ensuring that computers with covered data are identified and procedures followed to ensure the security of that data during its life cycle in MSL's possession or control.

Monitoring and Testing: Monitoring procedures will be used to regularly test and monitor the effectiveness of information security safeguards to ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security.

Service Providers: During business, MSL may from time to time appropriately share covered data with third parties. Such activities may include collection activities, loan servicing, payment plan providers, credit card processors, transmission of documents, destruction of documents or equipment, or other similar services. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that can maintain appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

Responsible Organization/Party: Assistant Dean Sullivan and Assistant Dean Kaldis shall serve as the Coordinator of the Plan, with the Director of Technology Mick Coyne and Director of Library and Information Services Daniel Harayda, as well as other School Officers as needed, as well as other School Officers as needed.

Enforcement: Each Department is responsible for overseeing the enforcement of the policy in their departments. The Director of Technology, Mick Coyne and Director of Library and Information Services Daniel Harayda are responsible for notifying Department about changes to the policy. If a violation of this policy occurs, The Director of Technology Mick Coyne and Director of Library and Information Services Daniel Harayda will lead an investigation about identified security breaches and may terminate access to protected information of any users who fail to comply with the policy.

Related Policies, Laws and Resources: The Federal Trade Commission (FTC) has stated that colleges and universities are considered in compliance with the privacy provisions of GLBA if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). MSL has adopted comprehensive policies, standards, and guidelines relating to information security, including FERPA. Other related policies (www.MSLaw.edu) are incorporated by reference into this Information Security Plan.

Breach Reporting of Student Financial Aid Data: E-mail cpssaig@ed.gov, Jackie at FAS (jackie@fasinc.net) and Mick Coyne, Director of IT. Include in the e-mail:

- Date of breach (suspected or known) Impact of breach (number of records, etc.);
- Method of breach (hack, accidental disclosure, etc.);

- Your third-party security details and point of contact.
- E-mail and telephone details.
- Remediation status (complete, in process —with detail);
- Next steps (as needed)

Disaster Recovery

Massachusetts School of Law Disaster Recovery Plan and IT Procedures:
In the event of institutional closure, MSLAW will, at a minimum, observe the procedures stated in the New England Commission of Higher Education (NECHE) document entitled, "Considerations When Closing an Institution of Higher Education", as well as the closure guidelines of the Massachusetts Department of Higher Education for Independent schools, including the identification of another entity to preserve and safeguard student records so that those records will be available for students to obtain. Information for students and potential students about obtaining records from closed institutions can be found on the websites of the Massachusetts Department of Higher Education and NECHE.

In the event that MSLAW decides to discontinue its program before all enrolled students have completed their program of study, MSLAW will implement a teach-out plan in accordance with the requirements of its accreditor, NECHE.

The IT Disaster Recovery Plan for MSLAW sets the direction and priorities on how the MSLAW IT team will proactively protect MSLAW IT assets prior to a disaster; how best to operate during and after a disaster; and, how best to protect the mission critical services that will provide MSLAW with the best chance of moving forward as quickly and successfully as possible. MSLAW creates and manages large volumes of electronic information and data. Those records are vital to the continued operation of the business during a disaster. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential. The MSLAW IT Infrastructure Team including its Infrastructure Emergency Response Team (IERT) is the group that supports this plan.

The IERT determines which servers, storage, networks, software licenses, business application, and databases are maintained and will be required for recovery such that downtime from a disaster is minimized.

Data Backups and Offsite Storage of System Backup Media
We have implemented robust enterprise-wide backup solutions to include daily, weekly, and monthly data backup, archive and recovery that are an integral part of the IT disaster recovery plan. IT has developed a data backup strategy that begins with identifying and classifying the data to backup, which data must be archived offsite, selecting, and implementing a robust backup solution, scheduling, and conducting backups on a daily, weekly and monthly rhythm and periodically validating that the data backups have been accurately backed up with no corruption.

MSLAW Retention
MSLAW retains information in both hard and soft copy with full redundancy of that data. Off-site archiving is a necessity, and it originates from the file and server rooms. Archived backups are stored off-site in a secure environment. Data is retained on backup media and ultimately cycled through rotation for reuse.

Recovery Response Time
Recovery Response Time for MSLAW for data recovery is expected to be 30 minutes to hours depending on how much data needs to be recovered. System Recovery Time will range from one to three days depending on the extent of the problem. Servers and Workstations are backed up according to their use and extent of redundancy. Workstations are backed up to the extent that information is not maintained on the servers.

Network
The campus network is fully backed up on a daily basis and while there is some redundancy with other networks, the system is not fully redundant for all users so there will be periods where the network is not accessible to all users for periods ranging from a few minutes to multiple hours.

Telecommunication
The telephone system is partially redundant. In the event of a disaster, the MSLAW IT support personnel will assist with recovering the Voice-Over-IP (VOIP) system services and will coordinate with the system and support vendors.

Testing the Disaster Recovery Plan
The Infrastructure Emergency Response Team (IERT) is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan.

Remediating and Reporting Phishing/CEO Fraud

Get a Copy of the Email/Attempt:
Obtain a copy of the printed email with full headers and any original attachments. Revealing the routing information behind the email address will likely reveal the sender is not who they say they are. We take note of the IP address that the message came from. There are usually two forms of phishing in these circumstances: 1. The routing information has been falsified and the sender is 'pretending' to be someone in your network - the email address has been "spoofed" to look like a legitimate and trusted sender; 2. The information has not been falsified, and the sender is verified, but the actual email account has been compromised - an end user's desktop acting as a bot for the message or from a compromised or vulnerable server. We log this information internally and it becomes part of a report we file with the IC3.

Interview the Affected End-User:
Ask any and all end-users what happened, what they saw, and if they noticed anything strange or out of place before or after interacting with the phish.

Adjust email filters to block similar messages, notify other network users:
To prevent other users from falling victim to the same attack, we look for attributes in the email that you can filter out. In some cases, the From, Subject, and other fields may change. In the short-term, these identifying features can be used to blacklist more incoming attacks from the same user/server and can be set to filter these messages from reaching the domain again.

Log It:
We will check firewall logs for all of the suspicious IPs, URLs, etc., from the email, URL, attachment, etc. to see if there was any suspicious traffic entering/leaving the network going to those IPs.

Review Mail Server Logs:
Check to see which users received the message by searching your mail server logs, keywords, and key fields: the message ID, source IPs, From, Subject, file attachment name and type.

Review DNS logs:
Review and preserve DNS activity immediately prior to and after the attack. Ensure that your DNS, DHCP, firewall, proxy, and other logs don't rotate off. These logs are preserved for remediation and or legal purposes.

Change Passwords:
As a general rule of thumb, we will change the affected users' passwords — even if we determine that nothing serious happened and no sensitive information has been exfiltrated. If a user's credentials (especially those used for remote access) are compromised, an attacker could come back and use legitimate access and control methods. After passwords have been changed, we review and monitor the activity of the impacted user account for a period of time pre- and post-incident.

Use Attack as an Example:
We will use the event as an opportunity to raise security awareness among management and staff.

Quick-Hit Updates to MSL's Internet Security September 2023

Cyberattacks are a matter of "when," not "if." In response to the changing cyber threat-landscape and advanced persistent threats, MSL has adapted its information and network security environment with additional account and network hardening from Google, Dell's SonicWall, and VMWare Carbon Black.

- Google is one of the major industry leaders in internet-based services and is widely regarded for its account security and AI-based phishing detection. Google now provides MSL with 2 Factor Authentication (2FA) for all student, staff, and faculty email accounts, requiring all students, staff, and faculty to enter an additional six-digit key (sent via SMS) when logging into their accounts. In addition to this extra layer of security on all MSL email accounts, Google's email platform, GMAIL, also has specific email filter rules based on current and known phishing campaigns and fraud attempts and prevents 9/10 of those communications from reaching inboxes.

- VMWare Carbon Black is the NSA and CISA recommended and approved anti-malware/anti-ransomware endpoint client that is implemented on all staff and faculty machines to hunt threats, remove tracebacks, hijacks, and malware. Carbon Black uses its Defense-Grade level AI to predict threats to our network and our critical systems before they occur. Carbon Black will be paired with Google Workspace to provide authenticated logins for MSL staff and faculty while logging on to work off-site.

- Dell's SonicWALL has been a firewall mainstay in the internet security field for more than two decades, and after its acquisition by Dell, incorporated AI to become a next-gen enterprise firewall security. It now uses cloud-based algorithms and definitions to secure the incoming and outgoing internet traffic at MSL. Dell SonicWALL also provides Secure Remote Access, Email Security, Backup and Recovery, and Management and Reporting to organizations like MSL.