Midwestern University
Gramm-Leach-Bliley Act Summary Memo
Fiscal Year 2023

In 1999, the U.S. Congress passed the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999. It was signed into law as part of an effort to enhance competition in the financial services industry. The GLBA requires all financial institutions that collect financial information to take security measures to protect and safeguard sensitive data of their consumers. Higher education institutes that participate in federal aid programs are considered financial institutions under the GLBA, and the Federal Trade Commission (FTC) may find institutions that do not have GLBA safeguards in place in violation of the law.

The FTC published final rules related to the GLBA in 2000 and 2001 entitled Privacy of Consumer Financial Information and Standards for Safeguarding Customer Information, respectively. Key compliance requirements include designating an employee to coordinate an information security program, identifying risks to the security of customer information (including a risk assessment of computer information systems), and contractually requiring service providers to implement and maintain safeguards.

Updates to the GLBA went into effect June 9, 2023, which enhanced requirements around securing student information and protecting against threats. Additional requirements include enhanced monitoring of service providers, creation of a written incident response plan, and the requirement that a qualified employee report on information security risk and response issues to the Board of Directors.

Higher education institutions are deemed in compliance with the privacy provisions of the GLBA if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). Higher education institutions, however, are still subject to the provisions of the GLBA related to the administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue." (16 CFR 314.3)

The following information provides more information concerning the GLBA:

- Gramm-Leach-Bliley Act (Public Law 106-102)
- Privacy of Consumer Financial Information; Final Rule (16 CFR 313)
- Standards for Safeguarding Customer Information; Final Rule (16 CFR Part 314)

Midwestern University (MWU) complies with the GLBA by:

- Designating an individual to oversee customer information and to coordinate an information security program.
- Ensuring security and confidentiality of consumer information.
- Protecting against any anticipated threats, risks, and/or hazards to the integrity of consumer information.
- Protecting against unauthorized access to or use of consumer information that could pose a harm or inconvenience to the consumer.
- Assessing current customer information practices, identifying vulnerabilities, and taking appropriate measures to secure customer information.

- Performing an annual risk assessment and third-party tests and evaluations of security programs and prioritizing and implementing recommendations.
- Documenting policies, procedures, and roles. Maintaining a Disaster Recovery Plan which functions as an incidence response plan.
- Making an annual security presentation to the Board of Directors as well as regular security update presentations to leadership.

Midwestern University performs an annual risk assessment using the Clearwater Compliance product, IRMPro.

In 2022, Midwestern engaged the Burwood Group to perform a security audit to assess vulnerabilities, test our firewalls, and review existing policies. The University used the recommendations from this audit to improve systems and processes throughout the University.

As required by the GLBA, Midwestern also conducts annual external and internal penetration testing.

Also as required by the GLBA, Midwestern University management makes periodic presentations to the Board of Trustees to apprise them of the results of system security assessments and tests.

MWU uses two-factor authentication for many applications accessed from off-campus. MWU is also in the process of modernizing equipment across its IT infrastructure by retiring Avaya equipment and replacing it with state-of-the-art Cisco equipment and Cisco technology for increased network security.

MWU has determined that a crucial risk-mitigation strategy is educating and training the community. MWU administers a comprehensive data security training program that keeps its community informed and educated on information security.

Some key aspects and examples of that program are the following:

Data Security Awareness

Data security simply means keeping data protected from corruption, loss, and unauthorized access. At MWU, data security is an integral part of all solutions and services IT offers. IT uses internal tools and external resources to review and audit our systems, report on the current state of data security, and adjust to ongoing security threats to ensure relevant data is kept as safe as possible.

IT also continues to inform the community about current risks and mitigation strategies.

Our Lead Technology Specialist also provides in-service training to the Midwestern University community about cybersecurity. The training includes a variety of topics including cybercrime, malware, ransomware, bots, social engineering, and phishing and encourages the entire community to be a part of prevention. The training is available for viewing asynchronously on the HR website.

Data Security Awareness: Physical Security

Keeping data secure usually begins with a very simple concept: locks. Physical security is just as important as all of the other safeguards we use to help protect your data. It is easily implemented and only requires a bit of thought and perhaps an extra step from the customer:

- Make sure printed sensitive data and devices containing sensitive information are kept locked in the file cabinets. This would include flash drives, external hard drives, printouts, reports, and any other item that may contain sensitive or protected data.
- Be sure to lock your computer whenever it is unattended. This can be done quickly by clicking the Windows Key + L key or by simply logging out of your computer.
- Make sure your office is locked when you leave.

These simple physical security safeguards add another layer of security for your data.

<u>Data Security Awareness: Phishing emails</u>

Phishing email is an ongoing attack that affects most everyone with a publicly available email address daily. A phishing email is an unsolicited email sent to a recipient trying to get them to do “something” that will bypass their security settings. Phishing attempts have become more sophisticated where many phishing emails appear more and more like legitimate mail. Criminals have also generalized their message to bypass most phishing filters. Don’t get caught by phishing attempts by being aware of these warning signs.

The message is unsolicited and asks you to update, confirm, or reveal personal information (SSN, passwords, account numbers, etc.)

- The message has a sense of urgency (Do this NOW or you will lose access).
- The message has an unusual “From” address or an unusual “Reply-To” address (many times these addresses will not match with the alleged company requesting information).
- The website URL does not match the name of the entity that it allegedly represents.
- The message is not personalized or is personalized using your email address name (e.g., Dear jjacob:).
- The message contains grammatical errors.

Phishing Email Do’s and Don’ts:

- DO call the company to verify an email you may have received, however DO NOT use the phone number contained in the email.
- DO use common sense. If you have any doubts, DO NOT respond.
- DO NOT ever send credit cards, passwords, or other sensitive information via email.
- DO NOT click on the link in a suspicious email. Instead, phone the company or search/type the company web address manually to be sure you are going to the true web address.
- DO NOT open attachments from unknown sources. Many viruses and other malware arrive as an executable in an attachment.

The most common phishing email MWU currently sees are those that are asking for your login information along with some personally identifiable information. The best thing to remember is to NEVER give out your password to anyone for any reason.

In all phishing email cases, the sender will attempt to get you to divulge your information or click on a link using a sense of urgency (if you don't do this within x hours/days, something bad will happen) and appeal to something that you commonly use or want (PayPal payments, eBay auctions, package deliveries, invoices, etc.). MWU will never ask for your password information (or any other legitimate agency) via email. If you are unsure, please contact the support desk at 630-515-7361 or 623-572-3388 for further assistance.

The University reminds its employees frequently that it will never ask for employee password information (or any other legitimate agency) via email. If unsure, the University asks employees to contact the support desk at 630-515-7361 or 623-572-3388 for further assistance.

The University has added an easy way for employees to identify an email as a possible phishing fraud. At the top of each email, there is a button that can be clicked on if there is a suspicion of phishing, and when clicked the email is forwarded to IT security for further investigation.

Data Security Awareness: Ransomware Notice

An updated version of the Cryptolocker has recently been released dubbed "CryptoWall." This malware has been classified as ransomware, meaning the only way to recover your files without a backup will be to pay the requested ransom and hope that the criminals send you the keys or software to unlock your files (we DO NOT recommend that you do this).

This new variant is primarily activated through phishing emails and compromised websites. The author will try to get the user to click on a malicious attachment or go to a compromised website by either promising something highly desirable (click here to see the latest videos of <insert popular celebrity>) or utilizing alarming tactics (Thank you for your payment of $573.29 to <popular company>, click on the attached file to view your receipt). Once activated, the malware will proceed to encrypt all your data files effectively making them irretrievable.

You will eventually receive a message stating something to the effect that all your files have been encrypted. You must pay $xxx.xx within the next 72 hours to unlock these files or the unlock key will be forever destroyed." The malware will target any drive letter attached to your computer (i.e. flash drives or external hard drives that can be reached via a drive letter C:, D:, F:, etc.) which can cause complete and total data loss for that computer and anything attached to it.

Mitigation/Prevention:

- Do not click on links or attachments that you aren't expecting, no matter how dire the situation is being described.
- Maintain current backups of your data. Unplug the backup from your computer and store it in a safe location.
- Run and keep current antivirus and antimalware software.
- Keep your operating system and software up to date with patches.

Data Security Websites to visit:

- Facebook Security Tips
- Common Scams
- FTC - Keep PI Secure
- Check your Credit Reports Annually