ONU Information Security Program

Overview and Purpose

This program is designed to comply with the information safeguarding requirements of the Gramm-Leach-Bliley Act (GLBA) and well as the responsibility Olivet Nazarene University has to protect and safeguard the non-public information of its students and their families, its staff and others who have entrusted it with this information.

Non-public personal information ("NPI") is any personal information that cannot be found in public sources. Publicly available information would be details available from federal, state, or local government records; widely distributed media (such as telephone directories or newspapers); or information disclosed to the public as required by federal, state, or local law. NPI is usually obtained directly from the individual. It includes such details as the person's date of birth, social security number, financial account numbers and balances, sources and amounts of income, credit card numbers, and information obtained about visitors to your Internet web site, and sometimes could include home addresses and telephone numbers. (From Massachusetts Security Division, Summary GLBA http://www.sec.state.ma.us/sct/sctgbla/gblaidx.htm)

Policy

The University has adopted an Information Security Policy (reviewed April 2010) which addresses the University's response to GLBA. This policy also addresses the industry standard for data security as set forth in Payment Card Industry Data Security Standard (PCI-DSS).

Program Components

Compliance and best practice indicate the components are addressed in three areas:

1. Physical Security

2. Electronic Data Security (user)

3. Electronic Data Security (Information Technology) This program will be developed and administered within the department of Information Technology.

Physical Security

Physical Security is a combination of good business sense combined with an awareness of the particular environmental landscape. Each department will have varying degrees of risk to manage in order to put reasonable safeguards in place. There are several University departments which have a constant flow of students and visitors which would require more vigilance in the safeguarding of the information, while others rarely, if ever, have non-employees in their area. The following sets forth the general guidelines for physically securing NPI:

1. Computer screens where practicable should be oriented in a manner which cannot be easily read by passersby or other visitors. For example, computer screens in close proximity to doors or windows should not face the doors or windows. Angling them slightly will discourage both the curious as well as those with a malicious intent. There are screen visors and/or filters which would increase the difficulty for the casual or intentional observer to identify screen content.
2. Desks and other work areas should be cleared of NPI when no one is present for an extended period of time. Information should be visible only to the extent that it is necessary to perform your duties. Blank sheets of paper and documents flipped over can protect it from the casual eye. At workday’s end, any information should be returned to the desk, cabinet or vault.

3. NPI should be locked up when not in use and no one is present. At the end of the workday, all drawers, cabinets and vaults should be locked, even if it behind one or more locked doors. This step takes only minutes a week, but provides an additional reasonable safeguard.
4. NPI which is to be destroyed should be placed in a secure container for shredding or until it is shredded. An **unmarked** box under a desk emptied **daily** is a reasonable method to secure it until it can be disposed of effectively.
5. Any unnecessary duplicate copies of NPI should be securely disposed of promptly.
6. Access to NPI should be limited to those who have a need to know in the performance of their duties. This can be accomplished a number of ways, by limiting access to certain work areas, limiting keys to cabinets and vaults, and limiting by levels of viewing authority on the network system.
7. Unless there is a legitimate business need, NPI should not be taken from the department and/or off campus.
8. When an employee terminates, the Office of Human Resources, the Department of Technology Information, the Department of Public Safety, and if appropriate, faculty, staff and/ or students should be notified.
9. Only those employees who have been properly trained and authorized should handle calls and requests for NPI.
10. A current inventory of computers, laptops, PDA's portable storage devices and other equipment capable of obtaining downloadable information should be maintained. If the Department of Technology Information maintains the list for a department, a copy should

be provided to the department head or her/his designee. The use of flash, thumb or a USB for unencrypted storage of NPI should be prohibited.

11. A current record of keys issued to a department should be kept. If responsibility for maintaining this list is Physical Plant, a copy should be provided to the department head or her/his designee.

Electronic Security

1. A unique password is required to log onto a computer or any device which can access NPI. Additionally, any department specific or university specific (for example Datatel) should have an additional unique password.
2. Passwords should be required to be changed periodically, generally 180 days.
3. Users of computers should set up a time out feature which would require the screen to blank out and have the user log on to activate. The computer should also be "locked" when the user will be away from the computer for an extended period of time.
4. Users should log off computers and other devices at the end of the day.
5. Users should be limited to access information which is necessary for the performance their duties.
6. Most of NPI is stored on drives which are backed up daily by the Department of Information Technology. Users who have NPI on their computer's "C" drive should also back up externally no less frequently than daily. Backups should be stored at a remote location.

7. Users should not transmit unencrypted or non-password protected NPI. If a written or in person request is made to send via facsimile, care should be taken as to the legitimacy of the request and the facsimile destination before it is sent. (For example, on a request for a transcript to be sent to another educational institution, the facsimile number should be independently verified before it is sent.)
8. A user log should be maintained and should be reviewed for any unusual or exception activity. If the log is managed by the Department of Information Technology, the Department Head or her/his designee should be given a summary report of the findings, and if appropriate a copy of the report.
9. No hardware or software should be connected a University system computer or access device unless it has been first checked for viruses or other malicious software.

Electronic Data Security - I.T.

Network Management Team

To accomplish the goals of this policy, the Olivet Nazarene University network management team will perform the following functions.

1. Monitor network traffic, as necessary and appropriate, for the detection of network infrastructure problems, intrusions (internally and externally based), and network policy violations. If a security problem is identified, the network management team will seek the cooperation of the appropriate administrators or staff for the systems and networks involved in order to mitigate such issues. If necessary, the network management team will act unilaterally to isolate and contain the problem by isolating systems and their services from the network infrastructure, and promptly notify the appropriate resources when this is done.

2. Monitor and maintain campus infrastructure to allow compliance with university policies against pornographic and mature content via network connections. Traffic detected that violates these policies will be submitted to the office of Student Development.
3. Plan, implement, and review the results of network-based security scans of the systems and devices on university networks in order to detect vulnerabilities or compromised hosts. If detected security vulnerabilities, deemed to be significant risk to others, are not addressed in a timely manner, the network management team may take steps to disable network access to those systems and/or devices until the problems have been rectified.
4. Prepare reports of network security activities on a quarterly basis.
5. Provide security assistance and incident prevention advice to system administrators.
6. Coordinate all Olivet Nazarene University network security efforts and act as the primary administrative contact for all related activities. To ensure that this coordination is effective, security compromises should be reported to the network management team via e-mail at it@olivet.edu or telephone 815-928-5302.
7. Cooperate with Olivet Nazarene University departments (e.g., Student Development, Public Safety, Human Resources), state, and federal investigations into any alleged computer or network security incidents.
8. Cooperate in the identification and prosecution of activities contrary to university policies and the law. Actions will be taken in accordance with relevant university policies, codes, and procedures with, as appropriate, the involvement of the Public Safety and/or other law enforcement agencies.
9. Abide by a Code of Conduct for IT staff and administration.

System Administrators

System Administrators will perform the functions listed below:

1. Follow procedures and policies to protect the systems and services for which they are responsible.
2. Employ recommended practices and guidelines where appropriate and practical.
3. Cooperate with the network management team in addressing security problems identified by network monitoring.
4. Address security vulnerabilities identified by network management team scans deemed to be a significant risk to others.
5. Report computer/server security compromises to the network management team for assistance in tracking and containing intrusions.

The foregoing procedures described in this document are intended to be implemented University wide. Departments, to the extent necessary, shall put in place additional safeguards. The procedures listed above are to be reviewed no less frequently than annually.