INFORMATION SECURITY POLICY FOR OLIVET NAZARENE UNIVERSITY

Revision Approved: April 2010

This document has been developed in response to:

- A Federal Trade Commission (FTC) rule related to the safeguarding of customer information. The regulations under 16 CFR Part 314, published in May 2002 (May 23 *Federal Register* p. 346484), stem from the Gramm-Leach-Bliley Act (GLB), which mandates extensive new privacy protection for consumers. The GLB Act requires financial institutions, including colleges and universities, to take steps to ensure the security and confidentiality of customer records such as names, addresses, phone numbers, payment card account numbers, income and credit histories, and Social Security numbers. Plans and policies must be developed and established to protect such information.
- The requirements of the payment card industry as set forth in their data security standard (the PCI-DSS). This standard defines how merchants must handle customer payment card data and related sensitive information.

This document summarizes Olivet Nazarene University's response to such regulations.

The designated employee responsible for the coordination and execution of the information security plan is the Controller of Olivet Nazarene University. All correspondence and inquires should be directed to the Financial Services Office. The Registrar of Olivet Nazarene University is responsible for compliance with the Family Educational Rights and Privacy Act (FERPA). The Director of Information Technology is responsible for compliance with the PCI-DSS.

The following have been identified as relevant areas to be considered when assessing the risks to customer information:

Employee Management and Training
Information Systems
Managing System Failures
Computer Services/Information Technology
Student Loans
Registrar's Office
Financial Aid Office
Student Accounts Office
Residence Life and Student Development
Student Health Center
Financial Services
Human Resources
Business Office
Development Office
Academic Affairs
Graduate Education

The Financial Services office will maintain the information security program. They will provide guidance in complying with all privacy regulations. Each relevant area is responsible to secure customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes is maintained by each relevant area and made available to the Financial Services office upon request. The policies are reviewed on a yearly basis. In addition, the information technology department will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

Olivet Nazarene University will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Examples of contract wording may include:

1. an explicit acknowledgment that the contract allows the contract partner access to confidential information.
2. a specific definition of the confidential information being provided.
3. a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract.
4. a guarantee from the contract partner that it will ensure compliance with the protecting conditions outlined in the contract.
5. a guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information.
6. a provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract.
7. a stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract.
8. a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Olivet Nazarene University to immediately terminate the contract without penalty.
9. a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements.
10. a provision ensuring that the contract's protective requirements shall survive any termination agreement.

Olivet Nazarene University will conduct its business in a manner that is compliant with all current requirements of the PCI-DSS. These are outlined in Appendices A and B.

This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the university's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance and annual risk assessment shall be done by the Financial Services office.

APPENDIX A

ONU Policy Concerning Payment Card Data and Computer Systems

ONU will maintain a secure network :

1. We will maintain a campus firewall configuration to protect data from unauthorized access.
2. We will alter any vendor-supplied defaults for system passwords and other security parameters prior to placement of any system on the network.

ONU will protect cardholder data :

3. We will protect stored data from unauthorized access.
4. We will encrypt all transmission of cardholder magnetic-stripe data and sensitive information across our own network or any public networks.

ONU will maintain a vulnerability management program :

5. We will use and regularly update antivirus software on all campus computers.
6. We will develop and maintain secure systems and applications.

ONU will implement strong access control measures :

7. We will restrict access to payment card data to only those staff that have a need to know this information in the performance of their duties and for official ONU business.
8. We will assign a unique ID to each person with computer access.
9. We will restrict physical access to cardholder data

ONU will regularly monitor and test our network :

10. We will track and monitor all access to network resources and cardholder data.
11. We will regularly test security systems and processes.

ONU has adopted an information security policy

12. We will maintain a policy that addresses information security.

APPENDIX B

ONU General Policy Concerning the Handling of Payment Card Information

Who Should Know This Policy

Any official or administrator with responsibilities for managing University payment card transactions, and those employees who are entrusted with handling payment cards and payment card information.

Policy Statement

The University payment card handling policy requires each method of processing payment transactions be approved by the University Financial Services Office. The Financial Services Office will work in conjunction with Information Technology towards compliance with payment card industry data security standards. A quarterly scan of the network is required.

Each member of the campus community is responsible for the security and protection of electronic information resources over which he/she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise.

Responsibilities

The departments in possession of cardholder numbers and information should design adequate processes and procedures to ensure the following standards are maintained:

- Keep secure and confidential all cardholder numbers and information.
- Payment card receipts should typically be treated the same as you would treat large sums of cash. The department will be responsible for any losses due to poor internal or inadequate controls.
- Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data), cannot be stored in any fashion on computers or networks.
- Payment card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured fax, or through campus mail (sealed envelopes may be used).
- All documentation containing card account numbers must be maintained in a "secure" environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes.
- All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life (18 months) has expired.
- Restrict access to payment card data and processing to appropriate and authorized personnel.
- Establish appropriate segregation of duties between payment card processing, the processing of refunds, and the reconciliation function where possible. Supervisory approval of all card refunds is required.
- Perform a self-assessment, when requested, to ensure compliance with this policy and associated procedures, and report the results of this assessment to Financial Services.

- Notify the University Information Technology Security Office prior to implementation of any technology changes affecting transactions processing associated with the merchant account.

Establishing New Accounts or Agreements for Payment Card Acceptance
Contact University Financial Services before making any commitments to accept payment card data or transactions.