Information Security Program

Effective: 21 April 2023

1. Executive Summary

Olivet Nazarene University's Information Security Program addresses the responsibility the university has to protect and safeguard the private information of its students and their families, its staff and others who have entrusted it with this information. This policy is further designed to address Olivet's information security responsibilities under the following regulations and standards.

- Federal Education Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry - Data Security Standard (PCI-DSS)

2. Governance

The Information Technology (IT) Security team, under the auspices of the Chief Operations Officer (COO) coordinate efforts to implement this program. The IT Security Officer will report annually on the status of this program to the following entities, who oversee university compliance.

- FERPA: University Registrar
- GLBA and PCI-DSS: Controller, Board of Trustees
- Other: Chief Information Officer, University Data Committee, Director of Risk Management

3. Scope

For the purposes of this document, private information refers to any personally identifiable information that is not publicly available. This includes but is not limited to any of the following:

- Personally Identifiable Information (PII) as defined by FERPA
    - Any identifier (e.g. name, address, birth date, SSN)
      in conjunction with
    - the individual's education records
    - the individual's past, present or future physical or mental health or condition,
    - the provision of health care to the individual, or
    - the past, present, or future payment for the provision of health care to the individual
- Non-public personal information (NPI) as defined by GLBA
    - Social Security Number or alternate government identifier (collectively SSN)
    - Financial account status, balance or other details
    - Credit report
- Credit Card sensitive account data (collectively "PCI data") as defined by PCI-DSS
    - Primary Account Number (PAN)
    - Magnetic-stripe or chip data
    - Card verification code
    - PINs/PIN blocks

4. Program Components

Olivet's Information Security Program is addressed in four areas:

a) Physical Security
b) Electronic Data Security (Employee)
c) Electronic Data Security (IT Employees)
d) Electronic Data Security (IT Security)

Report any of the following concerns to the IT security team by e-mail at it@olivet.edu or telephone at 815-939-5302:

- Questions about your obligations under this program
- Questions about approved storage and processing of private information on university or third-party systems
- Storage or processing of private information inconsistent with this policy
- Changes that may affect the storage and processing of private information
- Suspected security compromises

4.a Physical Security

Employees with access to private information will:

1. Orient computer screens in a manner which cannot be easily read by passersby or other visitors.
2. Clear desks and other work areas of private information when no one is present for an extended period of time.
3. Lock up private information not in use or when no one is present.
    a. At the end of the workday, all drawers, cabinets and vaults should be locked, even those behind one or more locked doors.
    b. PCI data must not be stored on paper. If PCI data is received in physical form, it should be processed and destroyed immediately.
4. Protect private information until it is destroyed. An unmarked box under a desk emptied daily is a reasonable method to secure it until it can be disposed of effectively.
    a. All physical copies of NPI must be destroyed no more than two years after it is needed for business use or required by law to be retained.
5. Limit access to private information 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, or by appropriate access controls for computer systems.
6. Keep copies of private information in a secure location on campus.
7. When an employee is terminated, the Office of Human Resources, the Department of Information Technology, the Department of Public Safety, and if appropriate, faculty, staff and/ or students should be notified.
8. Not respond to calls and requests for private information without proper training and authorization.

4.b Electronic Security - All Employees

Employees with access to private information will:

1. Set a unique password for any account with access to private information.
    a. Passwords must not be physically written down.
    b. Passwords must not be shared with anyone. IT will never ask for your password.
    c. For additional information, see https://it.olivet.edu/index.php/self-help/passwords
2. Ensure computers and devices with access to private information are locked or signed out when the user will be away for more than 10 minutes.
3. Not store unencrypted private information.
    a. Employees must not store or process PCI data on any system without approval from Accounting.
    b. Storage of other private information should be restricted to locations approved by the University Data Committee.
    c. All electronic copies of NPI must be destroyed no more than two years after they are needed for business use or required by law to be retained.
4. Not transmit unencrypted private information.
    a. 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.)
    b. Private information should never be sent via email.
5. Only use approved third-party vendors to store and process private information.
6. Access only the private information necessary to perform their job. Any unnecessary access should be reported to IT and a supervisor for review.
7. Access private information only from a University-provided computer or device or from a connection protected by University-provided security software.
8. Abide by the IT Acceptable Use Policy.

4.c Electronic Data Security - IT Employees

IT employees will:

1. Employ recommended practices and guidelines where appropriate and practical. This includes, but is not limited to:
    a. Change default access controls such as passwords, SNMP settings, and other devices
    b. Install security patches for software and firmware
    c. Ensure correct system date and time for accurate monitoring
2. Develop software and systems that are free from known vulnerabilities.
3. Mitigate vulnerabilities and other security risks identified by the IT security team.
4. Report computer, server, and account security issues to the IT security team for assistance in tracking and containing intrusions.

4.d Electronic Data Security - IT Security

To accomplish the goals of this policy, the IT security team will:

1. Maintain awareness of current security threats, controls, and best practices.
2. Conduct a written risk assessment annually containing the following elements:
    a. Inventory of systems that store or process private information
    b. Evaluation of reasonably foreseeable risks and threats to private information

    c. Define criteria for selecting mitigating controls and accepting residual risk
3. Plan, implement, and review the results of network-based security scans of the systems and devices that store or process private information in order to detect vulnerabilities or compromised hosts.
4. Orchestrate penetration testing of systems that store or process private information.

To minimize the likelihood of an incident, the IT security team will:

5. Coordinate efforts to implement security patches for university systems.
6. Implement controls to minimize unnecessary access to university systems. This includes but is not limited to:
    a. Block untrusted network access to management of systems that process private information
    b. Limit communication to and from systems deemed end-of-life by the manufacturer
    c. Audit account access to university systems
7. Train users to recognize social engineering tactics and implement controls to minimize attacks attempting to exploit users.
8. Implement multi-factor authentication (MFA) or equivalent controls for account access to systems containing private information.

To reduce the impact of a potential incident, the IT security team will:

9. Implement controls to detect and remove malware from devices that store or process private information.
10. Monitor network traffic for infrastructure problems, intrusions, and policy violations.
11. Monitor user account activity to detect inappropriate access, intrusions, and policy violations.
12. Maintain an incident response plan designed to minimize the impact of potential incidents.
13. Maintain a business continuity/disaster recovery plan designed to minimize the impact of outages.

To maintain the good standing of the university, the IT security team will:

14. Coordinate all network security efforts and act as the primary administrative contact for all related activities. To ensure that this coordination is effective, the following should be reported to the IT security team by e-mail at it@olivet.edu or telephone at 815-939-5302:
    a. Suspected security compromises
    b. Storage or processing of private information inconsistent with this policy
    c. Changes that may affect the storage and processing of private information
15. Cooperate with university and law enforcement investigations into any alleged computer or network security incidents.

5. Annual Review

The IT Security Officer will perform an annual review of this policy and coordinate any changes or additions with affected parties as specified in “2. Governance” above.