FVI School of Nursing and Technology

Physical Facilities and Technical Infrastructure Operations and Maintenance Plan

Physical Facilities and Technical Infrastructure Improvement Plan

Purpose:

The purpose of this plan is to provide our employees, students, and guests with well-maintained and operational physical facilities and a technical infrastructure that will support the objectives of the institution. The institution is committed to improving and retaining physical facilities that provide support for the mission of the school and provide for the education of students. The technology infrastructure is and will continue to be tested for security and upgraded as necessary.

Goals and objectives:

The following goals and objectives have been developed in support of achievement of this plan:

1. Support of operational goals through verification of adequacy
2. Identify potential areas of improvement required
3. Identify personnel responsible for the improvement and adequacy
4. Ensure plan is maintained
5. Revise and publish updated plan as required

Activities:

The following outlines specific activities utilized the plan objectives:

1. Improvement of physical facilities and technical infrastructure resources are discussed during the annual budget meetings to identify and plan for upgrade and/or purchase of physical facilities and technical infrastructure.
2. The maintenance of physical facilities and technical infrastructure resources is discussed during the annual budget meetings to identify for the upgrade and/or purchase of the physical facilities and technical infrastructure.

3. There is coordination between the IT department and Facilities to ensure compliance with current regulations issued by the state and federal government.
4. Equipment maintenance and supplies are adequate to support facilities
5. Personnel are employed or contracted to maintain facilities, maintain the IT infrastructure, and make repairs and upgrades as needed.
6. Annual Fire Drills and Active Shooter Drills are performed.
7. Align physical facilities and technical infrastructure to ensure compliance with all relevant state, local and federal laws

Responsible Personnel:

The school's plan for the operation and maintenance of our facilities and technology includes assigned responsibilities as follows:

Personnel	Responsibility
Campus President (CP)	Approve budget for physical facilities and technical infrastructure.
Facilities Director	Attend budget meetings for all campus locations. Obtain approval from CP for budgeted expenditures. Coordinate implementation of approved expenditures.
Campus President (CP)	Responsible to manage the implementation of approved expenditures at campus level. Ensure provisions contained in building leases, such as parking lot maintenance, lawn care, and other areas such as maintenance and repair of air conditioning, plumbing/sewage, etc. are fulfilled according to contract. Communicate campus facility need to Facilities Manager.
Information Technology (IT) Manager	Communicate campus facility needs to Facilities Manager. Responsible for all aspects of the technical infrastructure including hardware maintenance, equipment leases, and software services.
Compliance Director/Facilities Director	Complete periodic audits to ensure safe, clean, and professional environment is maintained. Coordinate plan maintenance, update and publish as required.

Maintenance Timeline:

Physical facilities and technical infrastructure are reviewed annually during the budget meetings. This enables campus budgets to be reviewed by the Campus President and Board of Directors, to review, revise, and approve prior to the beginning of the next calendar year.

Budget allocations are provided for emergency repairs and maintenance. All faculty and staff are encouraged to submit requests for maintenance and upgrades.

IT provides comprehensive support in the areas of Application Services, Web Communications, User Support and Data Services. It is our mission to provide comprehensive and responsive support, technological expertise through close collaboration with all departments in realizing its goals and those of FVI.

Information Security Program

Information Security Program means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

As a postsecondary educational institution participating in the FSA programs, FVI School of Nursing and Technology is subject to the information security requirements established by the Federal Trade Commission (FTC) for financial institutions. These requirements apply to all students' information in the school's possession, regardless of whether the information pertains to the student, parent, or other individual with whom the school has a customer relationship or pertains to the customers of other financial institutions which provided customer information to FVI.

Designated Coordinator: Eusser Darling

Position: Information Technology (IT) Director

E-Mail Address: edarling@fvi.edu

Phone Number: (954)991-9011

Management Involved: Denyse Antunes /President

Richard Zaiden /Compliance Director

Lamar Haynes/Campus President

Gretel Chong/Campus President

Risk Assessment: FVI School of Nursing and Technology is aware of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of students' information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and has assessed the sufficiency of safeguards in place to control these risks. Intrusion assessment is ongoing. Protection layers are reviewed annually and up-graded as necessary.

Following guidelines as provided in 16 CFR S 314.4, the elements included in the institution's Risk Assessment process include:

1. Employee Training and Management.

2. Information systems, including network and software design, as well as information processing, storage, and disposal; and

3. Detecting, preventing and responding to cyber-attacks, intrusions, or other systems failures.

1. Employee Training and Management

In order to develop, implement, and maintain a comprehensive information security program accessible to all School constituents and contains administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the data it manages, the nature and scope of the School operations, and the sensitivity of any customer (student) information at issue, FVI School of Nursing and Technology implements ongoing training to its staff, faculty and students related to the institution's information security program.

As part of the employee onboarding process, individuals are required to complete within their first week an online video training session and assessments (NINJIO) provided before the start of the employee operation of their day-to-day activities. Training focuses on data breach incursions and how to prevent them, handling records and reporting procedures. The training continues by module as new modules are developed every month.

The main objectives of any and all training are aligned with the regulations as set forth in § 314.4 and are reasonably designed to achieve the objectives of section 501(b) of the Act to include:

(1) Ensure the security and confidentiality of customer information.

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer (student).

Evidence of employee training and management remains in the employee folder maintained in the Human Resources Office. In addition, all School personnel must read and sign the Information Technology manual of policies and procedures included in the Employee Handbook.

2. Information systems, including network and software design, as well as information processing, storage and disposal.

This is covered in the IT Policies during on boarding. As deemed necessary the IT Director will revise policies and communicate any revisions to all employees.

3. Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

Safeguards & Monitoring

FVI School of Nursing and Technology implements information safeguards to control the risks identified through risk assessment, and regularly tests and monitors the effectiveness of the safeguards' key controls, systems, and procedures.

Overseeing Service Providers

FVI may work with service providers. A service provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the school. FVI takes reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue and requires them by contract to implement and maintain such safeguards.

Evaluation & Adjustment

FVI evaluates and adjusts its information security program in light of the results of the monitoring, as well as for any material changes to daily operations or any other circumstances that may have a material impact on the school's information security program.

Preventing Copyright Violations

FVI maintains a zero-tolerance policy for any plagiarism and/or copyright infringements. The LMS includes scanning software that may detect plagiarism. The FVI school catalog addresses copyright issues.

Responding to attacks, intrusions, or other systems failures

- Risk assessments involve continuously evaluating threats, vulnerabilities and controls, and impacts on information assets, while risk management is designing, implementing, and monitoring safeguards as are necessary to protect the schools information technology. This document provides an overall framework or guidelines for performing a risk assessment to help develop a risk management plan.

Definitions:

Risk - possibility of suffering harm or loss

Asset - anything of value such as data, hardware, software, reputation, facilities, etc.

Threat - anything detrimental to the school's information assets

Vulnerabilities - weaknesses in a system, control or countermeasure that can be exploited

Impact - the consequences if a threat is successful

Safeguards for Identified Risks

The first part of a risk assessment is to classify what kinds of data the school has, and what types of protection are needed. The Information Security Program and the Confidentiality Policy define "confidential" and covered" data/information. Use the following matrix to determine the data classification.

	Confidential Data (Highest level of security)	**Sensitive/Critical (Moderate level of security)**	**Public (Low, but still some protection)**
Legal Requirements Industry Regulations	Protection of data is required by law (e.g., FERPA) or Industry Regulations	School has obligations to protect the data.	
Reputation Risk	High	Medium	Low
Data Examples	-SSN -driver's license info -Bank account info -Credit card info -income -tax returns -student records	-Information resources with access to Confidential Data -Contractual -Library transactions -Licensing restrictions -Facilities/controls.	-campus maps -personnel directory data -institutionally published data

Threats

Most threats will often fall into one of the following four categories:

- Malicious activity
- Malfunction
- Human error
- Environmental

Some specific examples include:

- Malicious activity
  - Cyberattacks
  - Equipment theft
  - Physical break-in
  - Social engineering
  - Eavesdropping
  - Self-replicating malware
  - Malware that requires user interaction
  - Malicious unauthorized access
  - Malicious unauthorized user
  - Malicious scan
  - Process violation
  - Physical attacks such as vandalism, looting, etc.
- Malfunction
  - Software malfunction
  - Hardware malfunction
  - Process malfunction
  - Power disruption
- Human error
  - Equipment loss
  - Miscommunication
  - Implementation error
- Environmental
  - Fire
  - Temperature and humidity extremes
  - Flood
  - Lightning
  - Damaging wind
  - Hazardous materials

Threat Agents and Motives:

A threat agent is the operative that exercises a threat to exploit vulnerability. A threat agent might be a human or a thing. Human threats are associated with a motive. The motive is the objective or reason for exercising a threat to exploit vulnerability. Motives can be intentional or accidental.

- Human
  - A person or group of people who are targeting systems might have motive to:
    - Data theft
    - System compromise
    - Political/business espionage.
    - Sabotage systems
    - Sabotage business processes
  - Employees can create vulnerabilities or cause exploits accidentally by
    - Not being sufficiently trained
    - Not following procedures
    - Being forgetful or distracted
- Natural or environmental agents
  - Weather - temperature extremes, humidity, damaging winds, or rain
  - Natural disaster - lightning, fire, hurricane, or earthquake
  - Equipment wear or defect - equipment damage or aging equipment
  - Corrosion - chemicals

Threat Probability:

Probable- Threat agent and motive exist and will exploit a vulnerability.

Possible- Threat agents and motive exist but are not likely to exploit vulnerability.
Unlikely- Threat agents are nonexistent or rare, so little or no threat danger exists.

Threat Impact: The compromise of sensitive information or a ransom situation**.**

Significant- If the threat exploits a sensitive or critical asset vulnerability, it could have a major impact on the academic or business goals of the institution.

Moderate- If the threat exploits a sensitive or critical asset vulnerability, it could have a noticeable, but not significant, impact on the goals of the institution.

Low- If the threat exploits a sensitive or critical asset vulnerability, the impact on the goals of the institution will be negligible or non-existent.

Status of Vulnerability Controls:

Not Protected- Adequate controls are not implemented to safeguard the vulnerability from likely or high impact threats.

Protected- Adequate controls are implemented to safeguard vulnerability from likely or high impact threats.

Not Applicable- Threats against vulnerability are not likely, will not have significant impact, or do not exist.

Unsure- It is not known if the vulnerability is protected.

Vulnerabilities and Controls:

General Categories for Strategic Vulnerabilities and Controls

- Policies, standards, procedures, guidelines
- Communication
- Records
- Risk
- Contingency

General Categories for Operational Vulnerabilities and Controls

- Access
- Change Management
- Environmental Protection
- Incident Response

Specific Example Categories for Strategic Vulnerabilities and Controls

- Policy, standards, procedures, guidelines
    - Creation, documentation, implementation, review and update
    - Compliance
    - Enforcement
- Communication
    - Hiring and screening
    - Expertise
    - Training and awareness
    - Coordination and collaboration
- Records
    - Logs
    - Documentation
    - Tracking and reporting
- Risk
    - Analysis
    - Verification
    - Mitigation
        - Balance of security with usability
        - Cost-effectiveness
    - Strategy
    -
- Contingency
    - Documentation
    - Testing

Specific Example Categories for Operational Vulnerabilities and Controls

- Access
    - Identification
    - Authorization
        - Data
        - Software
        - System and media
        - Workstation
        - Portable devices and media
        - Personally managed computers
        - Backups

        - Network
        - Location
    - Authentication
        - Session management
        - Passwords
        - Account management

Threat Probability continued:

    - Least privilege
        - Encryption
        - Trust
            - Account restrictions
            - File access restrictions
            - Software access restrictions
            - System access restrictions: PDA synchronization
            - Network segregation
            - Physical access restrictions
    - Disposal
- Change management: Planning and Vigor
- Environmental protection
    - Protection against critical staff outages
    - Temperature and humidity protection
    - Fire protection
    - Flood protection
    - Wind protection
    - Lightening protection
    - Protection from hazardous material
    - Power surge protection
- Incident response
    - Monitoring
    - Containment
    - Investigation
        - Forensics and evidence preservation

Risk Matrix – Institution’s documented safeguards for identified risks:

Using a risk matrix, we can attempt to quantify risk by estimating the probability of a threat or vulnerability being exploited to get an asset and assessing the consequences if it were to be successful. This will allow the prioritization of asset protection. See some random examples below:

5 (High Probability)					Credit Card
4			FA records	Ledgers	Student Grades
3	Student Information		Online Platform Activity		
2	Personnel Directory				
1 (Low Probability)					
	1 (Low Impact)	2	3	4	5 (High Impact)

Privacy Policy

What personally identifiable information is collected from you through the website fvi.edu, how it is used and with whom it may be shared.

Information Collection, Use, and Sharing

We are the sole owners of the information collected on this site. We only have access to/collect information that you voluntarily give us via email or other direct contacts from you. We will not sell or rent this information to anyone.

We will use your information to respond to you, regarding the reason you contacted us. We will not share your information with any third party outside of our organization, other than as necessary to fulfill your request, e.g. to ship an order.

Unless you ask us not to, we may contact you via email in the future to tell you about specials, new products or services, or changes to this privacy policy.

Your Access to and Control over Information

You may opt out of any future contacts from us at any time. You can do the following at any time by contacting us via the email address or phone number is given on our website:

See what data we have about you if any.

Change/correct any data we have about you.

Have us delete any data we have about you.

Express any concern you have about our use of your data.

Security

We take precautions to protect your information. When you submit sensitive information via the website, your information is protected both online and offline.

Wherever we collect sensitive information (such as credit card data), that information is encrypted and transmitted to us in a secure way. You can verify this by looking for a closed lock icon at the bottom of your web browser or look for “https” at the beginning of the address of the web page.

While we use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information.

The computers/servers in which we store personally identifiable information are kept in a secure environment.

Cookies

We use “cookies” on this site. A cookie is a piece of data stored on a site visitor’s hard drive to help us improve your access to our site and identify repeat visitors to our site. For instance, when we use a cookie to identify you, you would not have to log in a password more than once, thereby saving time while on our site. Cookies can also enable us to track and target the interests of our users to enhance the experience on our site. Usage of a cookie is in no way linked to any personally identifiable information on our site.

Sharing

We partner with another party to provide specific services. When the user signs up for these services, we will share names or other contact information that is necessary for the third party to provide these services. These parties are not allowed to use personally identifiable information except for the purpose of providing these services.

Updates

Our Privacy Policy may change from time to time and all updates will be posted on this page.

Contact Us

If you would like to learn more about our privacy policy, or to access your personally identifiable information contained on our website, you may contact us at:

FVI School of Nursing and Technology
3520 Enterprise Way
Miramar, FL 33025
By e-mail: itsupport@fvi.edu
By Phone: (954)6132900

You will be required to provide identification information to assure that this information is not released to others. We reserve the right to modify this policy at any time without prior notification.

IT Governance

IT will optimize value of investment in information technology by aligning IT strategies with institutional objectives. Strategic objectives in this context include goals established at the organizational level. IT will be transparent in its operations. Prioritization of work will be intentionally aligned with strategic objectives. IT will pursue leveraging existing services, where available. In the absence of existing services that accommodate the requirements, IT will analyze the build-buy-or-partner options. IT will increase efficiencies at quality control and managing assets through the adoption of automated solutions for the execution of regular administrative and asset management tasks. Such efficiencies will include enhanced capabilities at remotely managing, supporting, and inventorying devices across all campuses. IT will regularly evaluate processes and procedures in place to seek out efficiencies that can be leveraged through continuous improvement.

IT Security and Privacy

IT will follow industry best practices in ensuring information security and privacy. Measures at ensuring security and privacy will include, but not be limited to application security; server security; end-point device security; security of data at rest; security of data in transit; access control; and security-related user practices. IT protocol will continue to scan all devices for software updates and vulnerabilities, and systematically review system logs for auditing of security vulnerabilities. IT will promote awareness of security-related issues, as communicated through industry security notices and bulletins. IT will engage in an open and ongoing dialog with FVI staff about ways to maintain privacy and security of work and personal data. IT personnel will regularly undergo training on security matters, including sessions on systems security, web application security and data protection policies. All data managed through FVI systems will be classified and handled in accordance with federal and state guidelines. For risk mitigation, IT will provision and or recommend appropriate locations for data storage based on classification. IT will conduct periodic scans of managed systems for sensitive data and recommend appropriate action for data stored in unsanctioned locations. Written recommendations will be made for the removal of sensitive data that has been retained beyond business use.

IT Infrastructure

FVI will continue with the machine lifecycle replacement program. Regular reviews of the specifications for the standard machine replacement models will occur to promote use of quality, cost effective technology that leverages developments in industry. A process to identify resources-intensive operations and tasks across FVI, will be used to establish where special accommodations in replacement equipment are required (e.g., laptops for remote staff, higher computational resource needs, accessories, etc.). Specifications for higher-resource replacement computers will also be maintained to facilitate long-term financial planning throughout the IT lifecycle. IT will continue to support network and telephony services. IT will promote the use of collaboration technologies and will advocate for the availability of basic videoconferencing equipment for all staff for their workspaces. IT will identify standard collaboration technologies for use across the institution and encourage and facilitate their use by FVI staff. IT will also advocate for the establishment of collaboration workspaces across FVI that support videoconferencing. IT will continuously evaluate FVI server infrastructure and optimize it for changing needs. Changes include the need for additional resources, changes in technology and requirements, security enhancements, and revisions in data classifications. IT will work to identify valuable uses for enterprise-supported tools like Dropbox, Canvas, and Zoom in managing work and connecting with external constituents (e.g., students, faculty, staff, and the community).

Human Centered Support

IT will invest in the use of tools that facilitate efficiencies in providing end user support, including but not limited to tools that facilitate remote assistance, endpoint device management, and deployment of software updates and machine or software inventorying. IT will endeavor to always provide personalized quality customer service. IT will regularly communicate technology-related developments, global and local prevalent issues, opportunities, and training. A culture of welcoming feedback will be promoted and fostered. IT will regularly communicate about training opportunities and specialized training in software, general technology, and best practices. IT will take a proactive role in identifying opportunities where training may benefit all end users.

Investing in People

Through collaboration in design and implementation; intentional and self-initiated training; internal and externals conferences; and shared responsibility, IT staff will acquire knowledge in many different domains. Knowledge of how to execute any given IT task will be shared among several team members. IT will invest time in exploring new opportunities, learning new skills, sharing knowledge, and building and implementing innovative solutions for technology problems within FVI. IT will respect and encourage contributions from all team members in determining how best to solve problems and implement new tools, ideas, and approaches in support of FVI's team members and students.