4-OP-H-5 Information Security Policy

Responsible Executive: Finance and Administration

Approving Official: Vice President for Finance and Administration

Effective Date: May 1, 2020

Last Revision Date: 02/23/2016, Definition updates - 03/24/2020, Definition updates - 05/1/2020; 07/28/2020

I. INTRODUCTION

A. OBJECTIVE

The protection of Florida State University (FSU) data is critical to the University mission. Information security underpins the University's ability to be a good steward of the information entrusted to it by its students and employees, and by its extended community of patients, alumni, donors, volunteers and many others.

The FSU Information Security Policy establishes a framework of minimum standards and best practices for the security of data and Information Technology (IT) resources at Florida State University.

B. SCOPE

The Information Security Policy applies to all users of University IT resources, whether they are officially affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations. The policy applies to both University-owned computers (including those purchased with grant funds) and personally-owned or leased computers that connect to the Florida State University network. It applies to all devices that store FSU data. This policy applies to those who provide system, desktop, network, or other IT support, both Information Technology Services (ITS) personnel and University unit support staff. It also applies to those who partner with FSU to provide or receive services or information; therefore, contracts and agreements must include language whereby the contractor/partner agrees to comply with this policy.

C. DEFINITIONS

Availability – the principle that authorized users have timely and reliable access to information and information technology resources.

Confidentiality – the principle that information is accessible only to those authorized (authorized access).

Cryptography – the discipline that embodies the principles and methods for the transformation of data in order to hide semantic content, prevent unauthorized use, or prevent undetected modification. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way").

Data Owner – the head of a unit - dean, director, department head - who is ultimately responsible for that unit's data resources.

Data Manager – the unit employee(s) the data owner has delegated as operational oversight for the unit's data resources.

Encryption – the process of changing plaintext data into ciphertext through the use of a cryptographic algorithm for the purpose of security or privacy.

Integrity – the principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

Member or Member of the FSU Community – an authorized user of an FSU IT resource; includes faculty, staff, contractors, students, volunteers.

Private - data for which the unauthorized disclosure may have moderate adverse effects on the University's reputation, resources, services, or individuals.

Protected - data deemed confidential under federal or state law or rules, FSU contractual obligations, or privacy considerations such as the combination of names with respective Social Security Numbers. Protected data requires the highest level of safeguarding protection.

Spam - Unwanted and unsolicited email or material created or knowingly disseminated in such a large volume that it tends to disrupt the proper functioning of university information technology resources or individuals' ability to use such resources. Spam is most often sent to a large number of email accounts and may be used to deliver malware and/or links to malicious websites.

Public - data for which disclosure to the public poses negligible or no risk to the University's reputation, resources, services, or individuals; data that has been deemed public by state or federal law. This is the default data classification, and should be assumed when there is no information indicating that data should be classified as private or protected.

University Unit - defined by procedure 4-OP-H-5.1.

D. EXCEPTIONS

To request an exception for any provision of this policy, the University unit's Information Security Manager must first obtain approval from the unit's dean, department head, or director, and then send the approved request to the Director of Information Security and Privacy for determination. The exception request must be specific, include reasons for not complying with a provision, and the alternative control(s) to be adopted that will achieve the intended security goal.

E. CONSEQUENCES

Disciplinary action for violating this policy is governed under the University's Standards for Disciplinary Action for violation of provision of University Policy. Users who violate this policy may be subject to other penalties and disciplinary action, both within and outside the University. Additionally, independent of such procedures, the University may temporarily suspend, block or restrict access to an account or IT resources when it appears necessary to do so in order to protect the integrity, security, or functionality of University or other IT resources, or to protect the University from liability. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

II. POLICY

A. Chief Information Security Officer

The FSU Chief Information Security Officer (CISO) directs the Information Security and Privacy Office (ISPO) for the University. The CISO reports to the FSU Chief Information Officer and the Provost, and serves as the Chief Information Security Officer and the Chief Privacy Officer for FSU.

B. General Standards for All University Units

Information Security Manager

1. Each University unit and related affiliate organization shall designate an Information Security Manager (ISM) who will manage the unit's information security program. The dean, director, or department head of the unit will notify the Director of Information Security and Privacy of the ISM within 30 days of appointment.
2. The Unit ISM has the following duties that will be included in the position description:
    a. Maintain the unit's information security program according to the policy and guidelines promulgated by the ISPO,
    b. Immediately report suspected or confirmed computer and privacy incidents to the ISPO,
    c. Serve as liaison for the unit with the ISPO, and
    d. In coordination with the Unit Privacy Coordinator, ensure all unit staff receive information security and privacy training.

Protecting Data and Information

1. Any information, including e-mail messages or other data, produced, transmitted, or received by University employees "pursuant to law or ordinance or in connection with the transaction of official business" is defined as a public record by Florida Law, and is subject to the provisions of Chapter 119, Florida Statutes. Public records are subject to inspection and

copying upon request by any member of the public (except as specifically exempted by law), may not be deleted or destroyed except as authorized by law and must be retained according to retention guidelines published by the state of Florida. Nothing in the Information Security Policy should be construed to impair the public's access rights under Article I, Section 24 of the Florida Constitution, Chapter 119, Florida Statutes or other applicable state or federal law.

2. Each University unit bears responsibility
    a. To protect the confidentiality (authorized access), availability, and integrity of University information
    b. The levels of controls required to ensure that protections are appropriate are based on knowledge of what data the unit has
    c. and, classifying that data as protected, private, or public.

        The following standards support this effort and, unless otherwise stated, must be performed by each University unit.

        i. Every unit and individual must exercise due diligence to protect protected information.
        ii. FSU deans, directors, and department heads have direct operational-level responsibility for information management and are considered data owners.
        iii. In accordance with FSU Privacy Policy and Guidelines, each data owner or designated data manager(s) must maintain a reference list of the data and information collected, processed, transmitted, or stored by the units under his/her purview.
        iv. Only authorized individuals will have access to protected and private information.
        v. Authorization for access must be promptly removed when a user's University affiliation changes (e.g., reassigned duties, employed by a different unit, no longer employed, etc.).
        vi. Data owners or their designated data managers are responsible for authorizing access to information and must periodically review access rights to ensure validity.
        vii. Every unit must provide training on proper handling of information for workers whose duties involve contact with protected or private information or the IT resources that house protected or private information.
        viii. Encryption must be used to ensure authorized access when protected or private information is sent via email and when it is transmitted across the network.
        ix. Where technology permits and reliable key management practices are used to ensure against data loss, encryption may be used to safeguard protected or private information at rest.
        x. Wireless transmission of FSU data must be implemented using strong cryptography for authentication and transmission.
        xi. Mobile devices (such as portable hard drives, usb drives, smart phones, tablets, and laptops) that contain protected or private information must be encrypted.
        xii. When authorized by the applicable retention schedule, information, regardless of media type, must be destroyed; electronic data must be maintained in accordance with the same retention requirements that apply to the same data in non-electronic format.
        xiii. Computer equipment and information media (e.g., hard drives, thumb drives) must be sanitized prior to reassignment (e.g., wipe and then re-image) and must be sanitized or destroyed before disposal. (See NIST Special Publication 800-88, *Guidelines for Media Sanitization*)

Appropriate Use of Information Technology Resources

1. All FSU desktops, laptops, and mobile devices must employ a screensaver or inactivity lock of no more than 30 minutes, and require a password or pin for unlocking.

2. University computer users shall have unique user accounts.
3. Accounts that have administrator permissions must not be used as a user's default account.
4. All FSU computers must enable up-to-date anti-malware protection.

Contracts and Agreements

1. FSU deans, directors, and department heads must establish procedures to ensure contracts and agreements involving IT resources, cloud or other outsourced services, guarantee compliance with the FSU Information Security Policy.
2. When protected information is shared with non-FSU entities, agreements that specify appropriate use, storage, and eventual destruction of the information must be in place.

Risk Management

1. Each University unit will conduct an triennial risk analysis to evaluate the information security and privacy status of the unit.
2. Each University unit will provide the analysis results to the Chief Information Security Officer in ISPO.
3. Based on the results of the risk analysis, the University unit will develop a mitigation plan to correct deficiencies.
4. The ISPO will develop guidelines and tools to help units with the risk analysis process.

University units must develop and maintain a written business continuity plan that provides information on recurring backup procedures, and also recovery procedures from both natural and man-made disasters.

C. General Standards for All Individuals

FSU provides a wide variety of IT resources, including computers, networks, software, computer accounts, cellular phones, office telephones and hand-held/wireless devices, for use by University students, faculty, and staff. These resources are administered by the Information Technology Services, schools, colleges, departments, and institutes, and are intended for the legitimate business of the University. User accounts and IT resources provided to faculty, staff, and students of FSU come with the associated responsibility to abide by University policies and procedures, state and federal laws and rules, and other applicable contractual obligations (such as PCI-DSS).

This policy should not abridge academic freedom, constitutional guarantees of free speech, or freedom of expression; rather, this policy contributes to the protection of these ideals by helping reduce risks of unauthorized access and modification of information, ensure appropriate availability of information, and protect individuals' privacy. In addition to consideration of legal liability issues, the institutional image and reputation of FSU as a major research institution are valuable assets requiring protection.

Each member (faculty, staff, contractors, students, and certain visitors) of the FSU community and anyone who connects a device to the FSU network is responsible for the following.

Compliance

1. Each member of the FSU community (subsequently referred to as member) is responsible for complying with FSU security policies and procedures when performing University work or when using University information technology resources.
2. Each member must comply with applicable state and federal information security laws and rules, and with contractual obligations (e.g. Payment Card Industry Data Security Standards).
3. Unauthorized or fraudulent use of University computing resources may result in criminal prosecution.
4. The University may remove a website from any FSU server if the website is found to be in violation of federal, state, or local laws or rules, or FSU rules, policies or procedures (including this policy).
5. The University reserves the right to contain security exposures due to devices that are:
    a. imposing an exceptional load on IT resources (e.g., email spamming, network denial of service);
    b. disrupting the network;

c. exhibiting a pattern of malicious network traffic scanning or attacking others;

d. exhibiting behavior consistent with compromise.

Monitoring of University IT Resources

1. To help secure the infrastructure and in response to malicious activity to ensure effective mitigation, the FSU ISPO may perform or authorize network security monitoring, intrusion detection/prevention, website scanning, network scanning, and other security procedures. Use of FSU information technology resources constitutes consent to monitoring activities.
2. To support public safety incidents and health emergencies and consistent with applicable privacy law and policy, FSU may perform monitoring, including but not limited to, location data, wireless connections, and FSU card utilization. Use of FSU information technology resources constitutes consent to monitoring activities.

Data Protection

1. Each member must ensure University data stored on workstations and other devices or locations under the user's control (as opposed to a regularly backed-up shared directory) is routinely backed up.
2. Protected and private information sent via email must be encrypted.
3. Logoff or lock the workstation prior to leaving the work area (Windows shortcut: Windows+L and on a Mac CTRL+Shift+Eject/Power).
4. Personal device use cannot be avoided in the University environment; however, it does pose risks (e.g., data leakage, malware introduction, unauthorized access). Members of the FSU community must exercise caution to protect and secure their personal devices that are used on the FSU network or that store University data.

Network and Device Protection

1. Owners of devices that connect to the FSU network must comply with the following:
    a. All computers and other devices capable of running anti-malware software must employ licensed and up-to-date anti-malware. Failure to do so may result in revocation of network access;
    b. All computers and other devices must have up-to-date security patches;
    c. Owners must ensure default and vendor-supplied passwords are changed.
2. All individuals (and departments) are prohibited from running any service or device which disrupts or interferes with the FSU network.
3. The installation of network devices must be approved by ITS Network Services. This includes, but is not limited to: hubs, routers, switches, remote access devices, modems, wireless access points or any other devices that allow access to the FSU network.

Accounts and Passwords

1. Members must not share FSU accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.
2. Each member is accountable for activities performed by his/her account.
3. VPN (Virtual Private Network) accounts may not be shared.
4. Members must use a long complex password where possible.
5. Immediately report suspected account compromises according to **incident reporting procedures (https://its.fsu.edu/sites/g/files/upcbnu1011/files/ISPO%20Pages/FSU%20Incident%20Response%20and%20Repo**
6. Immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to incident reporting procedures.

Personal Use

1. Personal use of University IT resources,
    a. must not interfere with the performance of the member's job duties or other FSU responsibilities;
    b. must not result in additional cost to the University;
    c. must not consume significant amounts of IT resources (e.g., bandwidth, storage);
    d. must not violate this policy.
2. Individual University units may implement additional limits on personal use of University IT beyond the parameters in this policy. Any additional limits must be documented by the unit and shared with unit members and the Information Security and Privacy Office.

Inappropriate Use

1. Inappropriate use of FSU email includes, but is not limited to, the following:
    a. auto-forwarding FSU business emails to a non-University email address;
    b. Impersonating another person;
    c. distribution of malware;
    d. forging email headers;
    e. Propagating "chain" letters, spam, junk mail, etc.
2. Members may not use University IT resources for the following:
    a. personal financial gains (e.g. running a business) or non-FSU commercial purposes;
    b. accessing or viewing pornographic or obscene materials unless necessary and approved for academic instruction or research;
    c. impersonating another person or misrepresenting authorization to act on behalf of others;
    d. engaging in activities that may harass, threaten, or abuse others;
    e. stating or implying without authorization, that the member is acting on behalf of the University;
    f. utilizing the University's trademarks or logos without specific authorization from the FSU Office of University Trademark Licensing;
    g. performing actions that violate copyright laws;
    h. illegally duplicating software (Computer users should be able to prove ownership of software in their possession);
    i. any activity which may adversely affect the confidentiality, integrity, or availability of IT resources or data.
3. Members must not delete or destroy public records without authorization
4. Members must not disable, alter, or circumvent FSU device or network security measures.
5. Members must not attempt to access IT resources or information for which they are not authorized.
6. Monitoring, sniffing, and related security activities shall be performed only by authorized workers based on job duties and responsibilities, by members authorized by the Director of ISPO, or unless necessary for academic instruction or research and approved by the director of the unit that supports the system.

D. General Standards for IT Management and Operations

The FSU mission depends on a reliable IT infrastructure and competent and responsible IT workers. Only through security-conscious IT management and operations can we ensure the FSU IT infrastructure is as secure and resilient as it can be.

Information Technology Workers and Accounts

1. ITS and University units that employ IT workers shall provide training for those workers to ensure competency in both technical and security aspects of their positions.
2. Information technology workers shall be granted access to University information technology resources based on the principles of "least privilege" and "need to know."
3. ITS and University units shall establish procedures to ensure administrative rights for information technology resources are restricted to information technology workers who have received appropriate technical training and who are authorized based on job duties and responsibilities.
4. Interactive administrative accounts must not be shared and activities using administrative accounts should be traceable to an individual.
5. Service accounts (e.g., backup) must not be used for interactive sessions.

Physical Security for IT Resources

1. Physical access to central information resource facilities (e.g., data centers and communication closets) must be restricted to authorized personnel.
2. Physical IT resources are to be protected from environmental hazards (e.g., temperature, humidity, dust, etc.) in accordance with manufacturers' specifications.

Information Technology Maintenance

Information technology personnel and teams must abide by these standards to ensure the FSU IT infrastructure is as secure and resilient as it can be.

1. Identify and document all IT resources within her/his purview.
2. Implement a patch management process for IT resources and software.
3. Ensure up-to-date anti-malware is maintained on IT resources.
4. Monitor resources to ensure desired performance and facilitate capacity planning.
5. Regularly review system activity logs.
6. Document configurations of network devices (routers, switches, firewalls, IPS/IDS, modems, etc.).
7. Maintain up-to-date network diagrams.
8. Implement a change management process to ensure proposed modifications to configurations are reviewed, approved, tracked, and documented.
9. Ensure all network device installations are coordinated and approved by ITS.
10. Monitor for unauthorized wireless network access points.
11. Upon detection, remove unauthorized wireless access points connected to the FSU network.
12. To prevent data loss, key management processes must be in place and documented prior to encrypting data at rest.
13. Administration of hardware, software, or applications performed over a network shall be encrypted (where technology permits).
14. Ensure data, devices, networks, and process required for specific types of data or functions (such as credit card processes) comply with the related standards (e.g., PCI-DSS).
15. Document standard hardware and software to be used in the staff-network environment.
16. Document standard configurations to be used to harden IT resources.

17. FSU wireless environment must not use vendor defaults (e.g., encryption keys, passwords, SNMP community strings, etc.).
18. Ensure network perimeter security measures are in place to prevent unauthorized connections to University IT resources.
19. Document IT resources and associated owners and custodians.

IT Infrastructure Security

1. Where possible, auditing should be implemented so audit records can trace actions to users so they can be held accountable.
2. Implement procedures to protect the integrity and authorized access of audit logs.
3. Log files and audit records must be retained as required by related State, Federal, or contractual (e.g., Payment Card Industry) schedule.
4. Information technology systems and applications should be analyzed prior to production implementation and regularly thereafter to ensure security controls are appropriate.
5. Information technology resources identified as critical to the continuity of University operations shall have documented disaster recovery plans providing for quick resumption of critical functions and the eventual return to normalcy for IT operations.
6. Through the use of backup, replication, high availability, or other technology, data and software essential to the continued operation of critical University functions must be recoverable.
7. The development and test infrastructures shall be physically or logically separated from the production infrastructure.
8. Databases and files containing critical, protected, or private information shall be placed in an internal network zone segregated from the Internet-facing network segments.

Application Development

1. Production data must be protected.
2. Production data classified as protected or private may be used for testing/development if:
    i. the data owner authorizes the use;
    ii. test system security controls provide for restricted access and auditing;
    iii. the production data is removed from the system when it is no longer required.
3. Technology managers shall restrict and tightly control the use of utility programs that may be capable of overriding system and application security controls.
4. Application security should be addressed throughout the application procurement process and/or application development lifecycle.
5. The application (data) owner is responsible to define the security-related business requirements (e.g., identification of protected data, specifications of groups or users who will be authorized access); based on these requirements, the application development team will implement appropriate controls.
6. The development team also will implement appropriate controls to minimize risks to the IT infrastructure and other IT resources.
7. Applications that house protected data should have processes for tracking the access and modification of protected data.
8. Application security documentation shall be maintained and be available upon request to the ISPO.

III. LEGAL SUPPORT, JUSTIFICATION, AND REVIEW OF THIS POLICY

Specific Authority

BOG Regulation 3.0075 Security of Data Related Information Technology Resources Florida Statutes

Chapter 501.171, Security of confidential personal information

Family Educational Rights and Privacy Act (FERPA)

Health Insurance Portability and Accountability Act (HIPAA)

Payment Card Industry Data Security Standard (PCI DSS)

4-OP-H-5.1 Defining University Units

Responsible Executive: Finance and Administration

Approving Official: Vice President for Finance and Administration

Effective Date: May 1, 2020

Last Revision Date: Unrevised at this time

The Vice President for Finance and Administration and the University Provost, or other University executive management they delegate, will identify University units that provide business functions that if disrupted could impede the university's ability to meet its mission and/or strategic goals, could have a major financial or reputational impact, or could result in significant regulatory or contractual non-compliance, required to maintain a Business Impact Analysis, Disaster Recovery Plan and Risk Assessments on a triennial basis.

Each University unit identified to maintain a Disaster Recovery Plan will exercise the plan on an annual basis, document lessons learned, and develop remediation steps to address plan weaknesses.

Procedure for Defining University Units (/sites/default/files/media/doc/4-OP-H-5.1%2020%20Procedure_Defining_University_Units.pdf)