Unit Information Security Manager

Information Technology Services (ITS)

Information Security and Privacy Office (ISPO)

July 2018

Version 1.0

The Information Security Manager (ISM) manages the university unit's information security program.

ISMs help university unit faculty, staff and management comply with the FSU Information Security Policy, applicable grant requirements and any other information security requirements affecting the university unit.

The dean, director, or department head assigns the ISM role. While the IT Manager often is named ISM, that is not always the case. The person designated as the ISM is generally considered to be the *data custodian* for the university unit and should have a thorough understanding of how data is stored and maintained.

This document covers the basic functions of the ISM as outlined in the FSU Information Security Policy 4-OP-H-5.

Policy Requirements for the ISM:

The FSU Information Security Policy 4-OP-H-5 states the following:

II. POLICY

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 university unit's information security program. The dean, director, or department head of the university unit will notify the Director of Information Security and Privacy of the ISM within 30 days of appointment.

2. The University unit ISM has the following duties that will be included in the position description:
    a. Maintain the university 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 university unit with the ISPO, and

    d. In coordination with the Unit Privacy Coordinator, ensure all university unit staff receive information security and privacy training.

The following are detailed examples of the duties of the ISM:

A. Maintain the university unit's information security program according to the policy and guidelines promulgated by the ISPO.

ISPO has developed an Information Security and Privacy Plan. This is the plan that FSU is following to implement a framework of safeguards to protect the Confidentiality, Integrity and Availability (CIA) of data and information resources.

- FSU Information Classification Guidelines
- Contract Addendum for University Sharing of any Information Classified as Protected and Private with a 3rd Party Vendor or Service Provider
- FSU Incident Response and Reporting Procedures
- OneDrive Data Use
- Information Security Manager
- Unit Privacy Coordinator
- Guidelines for the Use of Personal Cloud Services for University Business
- Practice Secure Programming
- Guidelines for Faxing FSU Classified Information as Protected
- Nexpose User Guide - Contact ITS/ISPO at ITS-SecurityOps@fsu.edu
- Guide to permanently sanitize media
- Guide to DDoS Attacks
- Transport Layer Security Protection Cheat Sheet
- Reduce the Risks of SNMP Abuse

B. Immediately report suspected or confirmed computer and privacy incidents to the ISPO.

Through effective incident management, ISPO facilitates response efforts when cyber events occur. The following activities help minimize potential damage in the event of a security threat:

Incident Response and Reporting

ISM's should be thoroughly aware of the FSU Information Technology Security and Privacy Incident Response and Reporting Procedures. This document can be found here:

Information Technology Security and Privacy Incident Response and Reporting Procedures.

C. Serve as liaison for the university unit with the ISPO.

The ISM works with management, data owners, and Unit Privacy Coordinators within their university unit. The ISM also works with ISPO, and is expected to communicate ISPO related policies and procedures to university unit staff. Any university unit related questions, issues or procedures that need to be communicated to ISPO should be done through the ISM.

D. In coordination with the Unit Privacy Coordinator, ensure all university unit staff receive information security and privacy training.

The ISM should work with the Unit Privacy Coordinator to develop a security training program customized to meet the security requirements of the data the university unit maintains.

1. The FSU Information Security Policy requires the following:

    - Every university 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.

    - 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.

    - 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.

2. The FSU Information Privacy Policy requires the following:

FSU will make standardized information privacy training available to Unit Privacy Coordinators and the university in general. This training will provide appropriate privacy training for all faculty, staff and students.

3. **FSU Memo of Understanding Regarding Confidentiality:** A signed Memo of Understanding Regarding Confidentiality is required for FSU personnel with authorization to access or process protected or private information:

    - Each FSU position requiring access to protected or private information must be reflected in the position description.

    - For each person requiring access to protected or private information, signed Memo of Understanding Regarding Confidentiality must be maintained on file university unit and be available for audit. This information may be stored in a digital or paper format.

    - Employees designated as having access to select protected information (e.g., HIPAA) may be required to sign agreements acknowledging special confidentiality controls necessary to meet specific legal or contractual privacy requirements. These agreements are in addition to a signed FSU Employee Memo of Understanding Regarding Confidentiality document.

    - Each university unit must train its employees on the requirements to safeguard protected or private information. This training should occur prior to employee access of protected or private information or as required by legislation or contractual obligation.

    - As verification of participation, each university unit must maintain rosters of participants in online or in-person privacy training in an electronic or paper format.

FSU has several training resources available to the university units. The university units are free to utilize these resources and customize the use of these to best meet the requirements of each position.

A list of the training resources available include:

- Securing the Human at https://vle.securingthehuman.org
- Family Educational Rights and Privacy Act (FERPA)

  http://registrar.fsu.edu/records/ferpa/
- Florida Information Protection Act

  http://its.fsu.edu/sites/g/files/upcbnu581/files/legacy/information-security-and-privacy-office/training/Florida%20Information%20Protection%20Act%20of%202014%20%28FIPA%29.pptx
- Lynda.com
- Federal Virtual Training Environment (FedVTE) - FSU faculty and staff are able to create accounts on FedVTE to access online training components for IT security and privacy.

  https://fedvte.usalearning.gov/portal.php
- Health Insurance Portability and Accountability Act (HIPAA)

  https://www.healthit.gov/providers-professionals/guide-privacy-and-security-electronic-health-information
- Gramm-Leach-Bliley Act (GLB)

  https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
- General Data Protection Regulation (GDPR)

  https://one.fsu.edu/eu-privacy-policy

Additionally, ISPO has a training coordinator who will work with the university units to help develop an information security and privacy training program.