FSU Information Security and Privacy Office Charter

Mission

Privacy, together with 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 Florida State University Information Security and Privacy Office (ISPO) supports the University Mission of *maximizing excellence in all programs* by fostering information security and privacy approaches across all units of FSU. The goal of the ISPO is to implement a framework of safeguards to protect the confidentiality (authorized access), integrity, and availability of FSU information technology resources and information, and to ensure the University is able to meet statutory and regulatory obligations in a manner respectful of individual privacy.

Accountability

The Director of Information Security and Privacy manages the ISPO and is accountable to senior management through the Office of the Provost and Academic Affairs and the Associate Vice President/Chief Information Officer to:

- Establish the strategic direction of the ISPO;
- Ensure the continuous enhancement and effectiveness of the ISPO to present a proactive approach to information security at FSU;
- Promote information sharing throughout the University as well as among Florida's public universities;
- To provide a one-stop point of information and accountability for information security and privacy at FSU;
- Provide periodic assessments on the adequacy and effectiveness of the University's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.
- Report significant issues affecting privacy, including recommended process improvements, and provide follow-up on mitigation.
- Provide information on the status and results of campus unit security assessments and Privacy Impact Assessments.

- Coordinate with, and provide oversight of, other privacy compliance, control, and monitoring functions.

Independence

To provide for the independence of ISPO, the Director reports administratively to the University Provost and Associate Vice President and Chief Information Officer (CIO).

Scope

The scope of Information Security and Privacy comprises multiple focus areas: Policy, Training/Awareness, Incident Management and Response, Consulting, Assessments, Risk Management, and Survivability.

- The ISPO develops policies and guidelines to assist technology and information users understand their responsibilities.
- Through Training and Awareness initiatives, end users learn secure behaviors that support the protection of University, as well as personal, information.
- When security incidents or privacy breaches occur, quick and effective response is crucial to limit damage and quickly restore services. The focus area of Incident Management & Response supports this effort by promoting consistent means to prepare, respond to, recover from, and report incidents.
- The ISPO partners and consults with organizational units across the University to assist them in meeting their privacy and information security objectives.
- ISPO conducts information security and privacy assessments in accordance with approved plans and its established policies and procedures.
- Risk Management allows units to determine the risks that exist in their environments and how those risks can be reduced or eliminated.
- Survivability supports the planning for recovery of technology services following an emergency or system disruption.

The scope of information security centers on implementing appropriate technical, operational and management controls to protect confidentiality (authorized access), integrity, and availability of resources.

The information privacy scope of work is to determine whether Florida State University recognizes the risk associated with collecting and storing protected data and that the University is aware of and in compliance with applicable policies and laws. This supports:

- The expectation that personally identifiable information collected, processed, or stored by the University is protected from misuse or unauthorized access;
- Limiting personal data collection to only those data items required for legitimate business purposes;
- Respecting the rights of the data owners as guaranteed by laws, regulations, and contractual obligations;

- Confirming University organizations incorporate privacy procedures as an integral part of business system design processes;
- Significant legislative or regulatory privacy issues impacting the organization are recognized and addressed properly.

Authority

ISPO is authorized to:

- Have access to all functions, records, property, and personnel required for information security and privacy assessments.
- Make specific reports directly to the Provost, Associate Vice President of Information Technology and other entities as deemed appropriate.
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish information security objectives.
- When conducting risk reviews and assessments, obtain the necessary assistance of personnel in University units, as well as specialized services from within or outside the organization.

Responsibilities

ISPO has responsibility to:

- Maintain a professional staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this charter.
- Develop an information security strategy that presents a high-level plan for achieving information security goals.
- Research best practices and technologies that support information security.
- Establish a quality assurance program by which the Director assures the operation of ISPO activities.

Assessment and Advisory Services

The ISPO, in cooperation with the Office of Inspector General Services, conducts information security and privacy assessments in accordance with approved plans and its established policies and procedures.

The ISPO can also conduct independent information security and privacy impact assessments.

Assessment and Advisory services include:

- Developing a flexible annual plan in consultation with the Office of Inspector General Services using appropriate risk-based methodology, including risks or control concerns identified by management.
- Examining and evaluating the adequacy and effectiveness of the systems of internal privacy controls.

- Evaluating and assessing significant new or changing services, processes, operations, and controls coincident with their development and implementation.
- In coordination with the Office of the General Counsel and Office of Inspector General Services, assessing compliance with laws, regulations, contract/grant provisions, and internal policies, plans, and procedures.
- Reviewing operations or programs to ascertain whether results are consistent with established objectives.
- Performing consulting services, assurance services, to assist campus units in meeting privacy objectives.
- Evaluating emerging information technology audit/assessment trends and implementing best practices.

Risk Management Services

The focus area of Risk Management is the key to a successful information security program.

Information security is not exact or all-encompassing. No one can ever eradicate a// risk of improper, malicious or capricious use of information and resources. The goal of information security is that in a particular situation, the controls are commensurate with the value of the protected resource and weighed against the cost that would be incurred-financial or otherwise-in the event of unauthorized disclosure, degradation, or loss. The process of balancing risks, costs of protection strategies, and resource value is risk management.

Risk Management Services include:

- Partnering with University units to conduct risk reviews that highlight strengths and weaknesses of a unit's information security profile;
- Consulting with University units determine how best to minimize risk and protect resources;
- Directing assessments of critical program areas or new services to ensure appropriate security controls are in place;
- Perform network monitoring, intrusion detection/prevention, web scanning, and other security procedures to help secure the infrastructure and in response to malicious activity.
- Evaluating new and emerging security strategies and technologies for use in the University environment;
- Collaborating with the information security technology team to plan and implement the SANS Top 20 Security Controls.

Approved: Sally E. McRorie **Date:** 6-J.-J1

Sally E. McRorie
Provost and Executive Vice President for Academic Affairs
Florida State University