ISPO Cybersecurity Strategic Plan

2026 - 2029

Executive Summary

The Information Security and Privacy Office (ISPO) is committed to protecting Florida State University's digital assets and fostering a secure environment for academic and research excellence. This strategic plan outlines our proactive, risk-based approach to cybersecurity. Our core purpose is to safeguard the confidentiality, integrity, and availability of FSU's systems and data, thereby protecting the university from operational disruptions, financial loss, and reputational harm. By aligning our efforts with the university's mission, we aim to build a resilient and security-conscious community, ensuring that cybersecurity acts as an enabler of innovation, research, and learning across the institution.

Vision and Mission

- **Vision Statement:** To create a secure and resilient digital environment that empowers innovation in research and learning while protecting the entire Florida State University community.
- **Mission Statement:** The mission of ISPO is to protect FSU's information and technology assets from threats. We will achieve this through a comprehensive framework of risk-based safeguards, proactive defense, effective incident response, and community engagement, ensuring the university can meet its strategic, operational, and regulatory obligations.

Guiding Principles

Our cybersecurity program is guided by a set of core values that inform our decisions, priorities, and actions.

- **Mission Alignment:** Security and privacy will be implemented as integral components of the university's mission, designed to enable and support academic and research freedom.
- **Risk-Based Prioritization:** We will employ a strategic, risk-based methodology, aligning with the NIST Cybersecurity Framework, to focus resources on protecting the university's most critical assets against the most significant threats.
- **Shared Responsibility:** Cybersecurity is a collective responsibility. We will foster a culture where students, faculty, and staff members understand their role in protecting the university's digital environment.
- **Proactive Defense:** We will move beyond reactive measures by actively identifying and mitigating vulnerabilities, hunting for threats, and preparing for emerging cyber challenges.
- **Enablement and Collaboration:** Our goal is to serve as trusted partners and advisors, finding secure and efficient ways to support the innovative work of the FSU community.

Strategic Goals & Objectives

Our strategy is built upon seven foundational pillars that guide our operational priorities and define our path to success.

Goal 1: Bolster Cyber Resilience and Recoverability

Focuses on strengthening our defenses and ensuring operational continuity.

- **Objective:** Enhance proactive protection, prevention, detection, and response capabilities to safeguard FSU assets against emerging threats.
- **Objective:** Minimize the impact of cyber incidents through effective vulnerability management and rapid incident response.
- **Objective:** Ensure the continuity of university operations with robust disaster recovery planning and immutable backup solutions.

Goal 2: Enhance the University Risk Management Program

Focuses on maturing our ability to identify, assess, and manage risk.

- **Objective:** Strengthen FSU's overall cybersecurity posture and maturity through the alignment of strategy with industry-standard frameworks like the NIST Cybersecurity Framework.
- **Objective:** Strengthen governance by establishing clear roles, responsibilities, and oversight for cybersecurity across all university units.
- **Objective:** Mature the third-party vendor risk management program to ensure partners meet FSU's security standards.

Goal 3: Foster a Security-Aware Culture

Focuses on empowering the FSU community as our first line of defense.

- **Objective:** Increase cyber awareness across the university through targeted training, education, and continuous engagement.
- **Objective:** Enhance cyber and privacy training programs for all students, faculty, and staff.
- **Objective:** Expand the use of proactive cyber threat awareness tools to promote a vigilant and informed community.

Goal 4: Meet Security and Privacy Compliance Requirements

Focuses on ensuring adherence to all legal, regulatory, and policy obligations.

- **Objective:** Ensure and enhance compliance with all relevant IT security policies, standards, and legal requirements.
- **Objective:** Provide clear guidance and support to university units to help them meet their compliance responsibilities.
- **Objective:** Maintain a robust program to protect sensitive data types, such as payment card information (PCI) and research data.

Goal 5: Support Student Success and Career Readiness

Focuses on preparing students for a digital world and fostering the next generation of cybersecurity professionals.

- **Objective:** Provide students with cybersecurity knowledge and skills to ensure their safety and privacy online.
- **Objective:** Create and support co-curricular and career development opportunities in the field of cybersecurity.

Goal 6: Establish a Sustainable Financial Model

Focuses on optimizing resource allocation and demonstrating the value of security investments.

- **Objective:** Align cybersecurity investments with the university's highest-risk areas to maximize value.
- **Objective:** Actively work to reduce institutional costs associated with cyber liability and incidents.
- **Objective:** Ensure effective and transparent management of the ISPO budget and procurement processes.

Goal 7: Drive Cybersecurity Innovation

Focuses on embracing emerging technologies and methodologies to stay ahead of evolving threats.

- **Objective:** Continuously evaluate and adopt innovative cybersecurity technologies and forward-thinking strategies.
- **Objective:** Foster a culture of continuous improvement and adaptation within the cybersecurity program.

Governance and Oversight

Effective cybersecurity requires strong leadership and clear accountability.

- **Executive Sponsorship:** The Chief Information Security Officer (CISO) reports directly to the FSU Chief Information Officer (CIO) and the FSU Provost, ensuring that cybersecurity and privacy receive the highest level of management attention.
- **ISPO Leadership:** The CISO is the central point of contact and accountability for information security and is responsible for establishing the strategic direction of ISPO, implementing a framework of safeguards, and ensuring compliance.
- **Roles and Responsibilities:** ISPO, in partnership with Consolidated University Units (CUUs), has established clear responsibilities for key roles. These include the Dean/Director/Department Head (DDDH), the Information Security Manager (ISM) who ensures security and risk management plans are implemented effectively at the unit level, and the Privacy Coordinator who oversees the university's privacy program and manages privacy-related compliance.
- **Reporting:** The CISO reports on the university's security compliance, risk posture, and program effectiveness to executive management and the Board of Trustees.

Measuring Success

We will measure our progress and the effectiveness of this strategic plan through clear, outcome-focused metrics.

- **Key Performance Indicators (KPIs):**
    - Improve the university's overall cybersecurity maturity score.
    - Reduce time-to-detect and time-to-contain security incidents.
    - Meet target completion rate for mandatory cybersecurity and privacy training.

    - Reduce critical and high-severity vulnerabilities across university systems.
    - Meet ISPO's goals for our external cyber risk score and third-party security assessment rating.
    - Increase efficiency and security through proactive management of end-of-life technologies.
    - Meet ISPO's goal for the number of student interns participating in the internship and career development program.
    - Manage opportunities to reduce cyber liability premium through implemented security posture improvements.
- **Reporting:** ISPO is committed to providing regular reports on these KPIs and the overall state of the cybersecurity program to university leadership to ensure transparency and continuous improvement.

Conclusion: A Commitment to a Secure Future

This strategic plan is a living document that will guide our efforts as the digital landscape evolves. The success of our cybersecurity program does not rest solely with the Information Security and Privacy Office but is a shared responsibility across the entire Florida State University community. Through collaboration, vigilance, and a proactive commitment to the principles and goals outlined here, we strive to ensure our university remains a secure and resilient institution, empowering the groundbreaking research and academic excellence that defines FSU.