Information Security & Privacy Office Tactical Plan

Current Information Security & Privacy Services

The Information Security & Privacy Office (ISPO) provides information security and privacy program policies, standards and specifications that assist UNM in addressing the confidentiality, integrity and availability of Personally Identifiable and Sensitive and Protected Information (PII/ SPI). Services are defined as follows:

Information Security Incident Response The ISPO provides information advice, counsel, direction and support for responding to information security incidents. This includes incident and IT forensics examinations.

IT Security Assessments The ISPO provides information security assessments of business processes, projects, products, purchases and services, as well as information systems. These assessments include system penetration testing, security evaluation and vulnerability scanning.

Vision and Approach for Security and Privacy

The ISPO approach is to

- Work with academic and business units and UNM administration to develop and promulgate consistent, effective Information security and privacy practices in support of core IT services. In the event a department cannot incur the total cost to ensure secure practices, departments can leverage IT resources at a reduced cost to protect institutional information and systems
- Assist departments in applying information security and privacy principles to their IT environments to prevent incidents and breaches. This includes helping departments to identify, evaluate and mitigate information security vulnerabilities and risks
- Raise compliance issues to the UNM administration and recommend mitigation strategies
- Lead the state in information security and privacy practices for education and develop services to assist other members of the education community.

With this approach, UNM ISPO is a high value resource for our peers in the education sector throughout the state. ISPO’s vision for UNM security and privacy functions include

- The Chief Information Security Officer (CISO) has appropriate authority and resources to effect the changes needed across the institution not only to respond to security incidents and breaches, but also to mitigate the risks of incidents and breaches as part of a proactive vulnerability and risk management program
- The University has a Chief Privacy Officer (CPO) with appropriate authority and resources. The CPO has appropriate policies and programs in place to provide guidance to the Information Security practices of The University, and to improve UNM privacy practices to mitigate unauthorized disclosures of PII/ SPI
- Information Security and Privacy best practices are institutionalized and are readily available and understood in UNM and available as a resource to the community of New Mexico
• Information security and privacy practices are implemented across core services and across all areas that store, process, transmit PII/ SPI such that all employees who interact with PII/ SPI receive appropriate ongoing training, and have appropriate skills and knowledge to perform their assigned duties related to PII/ SPI

• PII/ SPI is always collected, stored, processed, and transmitted in an appropriately secure manner, providing the appropriate privacy and security protections to that information, and to the customers the University serves, cementing UNM’s role in leading the state in information security and privacy practices

Current Work and Issues Related to Existing Services

The Primary work of the ISPO continues to focus on the UNM Information Security and Privacy Programs, which primarily address the areas of Payment Card Industry (PCI), The Gramm–Leach–Bliley Act (GLBA), and The Health Insurance Portability and Accountability Act of 1996 (HIPAA) within the Enterprise Resource Planning (ERP) system, and securing the use of Social Security Numbers in UNM processes.

The ISPO is primarily engaged in responding to significant departmental security incidents and in providing advice and counsel in the institution regarding such incidents. ISPO capacity is severely stressed due to the reactive nature of the current environment.

Furthermore, attracting the skills and knowledge necessary to maintain an effective Information Security and Privacy Program is extremely challenging, given the premium the market places on such skills and knowledge, and the gap between that market premium and UNM’s salary structure. The ISPO has experienced 50% turnover in the last three years, and struggles to maintain a training budget large enough to develop and maintain necessary skills in house. Internal Audit findings also observed this resource gap.

12-24 Month Milestones

Summer 2015:
• Provide Security and Privacy direction for security-related IT projects: NetID password change automation; Data Center and Redesign subprojects; Banner XE subprojects: Single Sign on and Student and HR modules being deployed in first XE release; Multi-Factor Authentication (MFA); and Virtual Desktop Infrastructure (VDI)
• Provide updates to UNM Credit Card Policies
• Review security of UNM public facing web sites

Fall 2015:
• Information Security and Privacy Governance Group formed
• Migrate forensics servers into IT Data Center
• Introduce Phase I of ISPO Program to campus – Vulnerability Management Program
• Bring UNM Credit Card Processing into compliance with the industry standard in EVP Harris’ area by 11/1/15 and in the Provost’s area by 1/31/16
• Assist Data Governance in review of SSN use in core office areas

Winter 2015:
• Provide Security and Privacy direction for security-related projects, including the Oracle AIX to Linux project, and securing the Research Network
• Introduce Phase II of ISPO Program to campus – Event Management Program

Spring 2016:
• Provide Security and Privacy direction for security-related projects
• Re-write Enterprise Authentication and Authorization Applications
• Introduce Phase III of ISPO Program to campus – Security Awareness Program

**Summer 2016:**
• Security and Privacy direction for security-related projects: security specific technologies

**Winter 2016:**
• Review of security of UNM academic and business intranet web sites

**Spring 2017:**
• Comprehensive code review program for IT-managed services

**Summer 2017:**
• Comprehensive security logging and event management system for UNM