Current Information Security & Privacy Services

Information Security Services: The ISPO provides the following security services, some of which are “for fee.”

- **Forensics Consulting**: The ISPO assists authorized entities, such as Internal Audit, UNMPD, and HR in investigating allegations of computer-related policy violations.
- **Incident Response**: The ISPO assists departments that have experienced a security event or incident to help determine if a breach or other exposure has occurred, and to assist in institutional response to events, incidents, and breaches.
- **Security Scanning**: The ISPO provides security scanning of workstations, servers or network devices. This service is available for individual devices or for whole departments. Risk analyses can also be provided.
- **Security Assessment**: The ISPO conducts security and risk analysis of departmental computing environments on request.
- **Security Consulting for Projects and Initiatives**: The ISPO works with departments in establishing security deliverables for projects, including security hardware and software to help secure implementations.

In addition, the ISPO provides an Information Security Program of policies, standards and practices, including education, awareness and training materials that help departments address confidentiality, integrity and availability of information on UNM systems and computers.

Vision and Approach for Security and Privacy

Information Security group’s approach is intended to:

- Work with business units and UNM administration to
  - Evaluate the IT skills of departmental staff
  - Develop consistent, effective Information security and privacy practices in support of “common good” services. In the event a department cannot incur the total cost to ensure secure practices, they will be able to leverage IT resources at a reduced cost to protect institutional interests.
- Assist departments in applying information security principles to their IT environments to prevent information security and privacy incidents and breaches. This includes helping departments to identify, evaluate and mitigate information security risks.
- Raise compliance issues to the UNM administration.
- Lead the state in information security and privacy practices for education and develop services to assist other members of the education community. In this way, UNM Information Security and Privacy is a common good resource for our peers throughout the Education sector in the State.

Information Security group’s vision for UNM security and privacy includes:

- 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.
- 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 risks of incidents and breaches.
• Information Security and Privacy best practices are institutionalized and are available as resources for
departments who cannot ensure their own.
• Departmental IT staff receive adequate training, and have appropriate skills and knowledge to perform
their assigned duties, or central institutional resources are in place to provide secure IT services to those
departments.
• Sensitive and Protected Information is always stored, processed, and transmitted in the most secure
manner, providing the greatest privacy and security protections to that information, and to the
customers the University serves.

Statewide, higher education security and privacy network of resources to promulgate best practices in these
areas to peer institutions and their communities.

Current Work and Issues Related to Existing Services
Security and Privacy Programs
The Primary work of the ISPO continues to focus on the UNM Security program, focused primarily on the areas
of PCI, GLBA, HIPAA, and ITAR/ EAR Compliance.

In addition to the regular Information Security and Privacy events led by the ISPO, including Security and Privacy
Days for Students at the beginning of each semester, and presentations at Tech Days, the ISPO is focused on the
following for the Fall 2014 Semester:
• August, 2014: Policies and Standards Creation and/ or Revision including:
  o Information Security Program components:
    ▪ Data Center Standard
    ▪ Social Security Number Policy
    ▪ Credit Card Processing Policy (PCI) and Incident Response Plan
    ▪ Acceptable Computer Use Policy
• September, 2014: Hire Information Security Manager
• September, 2014: Updated on-line Information Security and Privacy Training
• September, 2014: Office of University Counsel legal Security and Privacy requirements checklist
• October, 2014: PCI Gap Analysis completed for type all Version 2 Self-Assessment Questionnaires (SAQs)
• November, 2014: Hire PCI Manager
• November, 2014: EAR, FISMA & ITAR compliance checklist developed
• December, 2014: Hire Information Security Analyst
• December, 2014: Direction for security-related projects:
  o Data Center and Network Redesign subprojects:
    ▪ Multi-Factor Authentication
    ▪ VPN increased security services

Disparate institutional business processes and security procedures, as well as the lack of appropriate skills and
training across UNM continue to impact UNM’s exposure to security risks. Many departmental business
practices have grown organically over time and would benefit from administrative and technical review. The
ISPO is primarily engaged in responding to significant security incidents and in providing advice and counsel in
the institution regarding these incidents. ISPO capacity is severely stressed in a crisis-dominated 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 75%
turnover in the last three years, and struggles to maintain a training budget large enough to develop the
necessary skills in house. The ISPO is challenged for resources in the areas of forensics security and in PCI, and
has made requests to the UNM administration for resources in this area. Internal Audit findings also observed this resource gap.

**12-24 Month Milestones**

- **Spring, 2015:** Standard enterprise PCI business solutions purchased, contracted and/or implemented³
  - Kiosk platform
  - Bookstore platform
  - Inventory sales platform
  - Telephone card swipe platform
  - Events management platform
- **Spring, 2015:** Direction for security-related projects:
  - NetID password change automation
  - Data Center and Network Redesign subprojects⁴,⁵:
    - Perimeter Network Firewall. Intrusion Detection and Prevention enhancements
    - Campus-wide NAT for workstations
- **Spring, 2015:** Banner XE security and privacy requirements⁸
- **Spring, 2015:** Review KSA recommendations¹
- **Spring, 2015:** Information Security and Privacy Governance Group formed¹
- **Spring, 2015:** PCI Version 3 SAQ Gap review
- **Spring, 2015:** EAR, FISMA & ITAR Program implemented¹
- **Spring, 2015:** Banner Database conversion from AIX to Linux security and privacy requirements⁸
- **Spring, 2015:** PCI Version 3 Gap recommendation¹
- **Spring, 2015:** HIPAA Gap Analysis completed¹
- **Summer, 2015:** Direction for security-related projects²,⁴,⁵
  - Research network implemented
- **Summer, 2015:** Information Security and Privacy Program Review¹
- **Summer, 2015:** HIPAA compliant central IT environment deployed⁴
- **Summer, 2015:** Direction for security-related projects:
  - Re-write of Enterprise Authentication and Authorization Applications
- **Summer, 2015:** Information Security and Privacy Program Policies and Standards framework developed and presented to UNM governance groups for feedback¹
- **Fall, 2015:** Comprehensive information security and privacy program finalized and approved¹
- **Spring, 2016:** Comprehensive review of security of UNM academic and business public facing web sites⁶
- **Spring, 2016:** Comprehensive review of security of UNM academic and business intranet web sites⁸
- **Summer, 2016:** Direction for security-related projects:
  - Data Loss Prevention and Internet segregation for business environments⁴,⁵

**Key Common Areas:**

1. Policies and Procedures
2. High Performance Computing Infrastructure
3. Purchasing and Contracting
4. Data Centers
5. Network Infrastructure
6. Common Help Desk Approaches
7. Customer Support
8. Education Technology Support