Information Security Consulting and Support

Release: 1.5 Date: 6/10/13
Owner: Enterprise Security Assurance

For further information or to request this service, please contact the AITS Service Desk at:

servicedeskaits@uillinois.edu
217-333-3102 (Urbana)
312-996-4806 (Chicago)

Service Description

Information Security Consulting and Support services are offered to help University departments safeguard University of Illinois data and meet the requirements of the University's security policies and other legal and regulatory requirements. These services help a University department to implement a quality information security program.

Benefits to the University include:

- Use of a standards based approach to security and risk management
- Increased understanding and awareness of information security matters that will improve an University Administration (UA) security posture
- Active participation in the integration of departmental level and UA level security processes

Services provided:

- Security consulting
  - Provide supporting analysis to help agencies resolve information technology risks, threats, and vulnerabilities and to implement adequate risk mitigation measures
  - Provide consultation to help UA respond to audit and/or security assessment findings
- Vulnerability and Penetration Testing
  - Scan network systems to discover Internet-exposed vulnerabilities
  - Scan web application servers for Internet and Intranet based vulnerabilities
- Incident Response and Investigation
  - Triage security incidents ranging from desktop compromises to system-wide issues
  - Provide coordination and consultation with University Counsel
  - Assist in preservation of data
  - Coordinate computer forensic services
  - Track current state of incidents
- Compliance and Audit Support

  - Provide guidance on implementing process controls on IT related activities to meet University compliance requirements
  - Support University Audit and External Audit inquiries related to IT controls
- Security manual development and ongoing review of UA policies, standards, and procedures
  - Assist UA with understanding and interpreting laws, regulations, University security policies and standards
  - Assist in development of departmental specific policies, standards, and guidelines to meet University policy requirements
- Security training and awareness activities and materials
  - Provide annual program of security training conferences and events for interested University of Illinois employees and consultants
  - Coordinate purchase and distribution of security training and awareness materials for use in UA
- Coordinate the required University's security liaison support role
  - Maintain University Security Contact (USC) information
  - Notify USCs of University of Illinois security matters
  - Provide authorized USCs with access to the security access request portals.
- Review UA projects and initiatives for adequate information security risk mitigation provisions
  - Review and/or manage UA projects/initiatives related to enterprise
  - security technology selection, licensing and centralized management
  - Review UA projects for appropriate risk mitigation measures, as part of the UA project management process
  - Review UA projects for appropriate security based on legal and regulatory requirements for data classification and handling
- Enterprise purchasing contracts for security related components
  - Evaluate security-related components of UA RFP and responses, including assist in interpretation of SAS 70s.
  - Perform data center security reviews for potential contractors.
  - Research and evaluate security technologies to identify strategic enterprise approaches for the deployment of security technologies that permit the University Of Illinois o benefit from standardization and economies of scale
  - Strategic planning for UA security needs
  - The following enterprise security software and tools are currently available for UA use:
    - Nessus Network Scanning
    - Appscan web-application scanning tool

Hours of Availability

- Standard business hours are 8:00 a.m. to 5:00 p.m., Monday through Friday, except for University of Illinois holidays
- On-call staffing is available for emergencies and after hours scheduled work
- In the event the UA seeks vulnerability or port scanning, the scanning activity will be conducted within the departmental's maintenance window unless other arrangements are made

- Emergency maintenance windows will be handled using the urgent change process

Customer Responsibilities

- Identify critical UA business systems and applications
- Implement University data classification, retention, and handling measures based
- on legal and regulatory requirements as required by statute
- Follow appropriate incident reporting procedures, including cyber security incident reporting as required by policies
- Follow standard processes and procedures for cyber security incident reporting
- Request and schedule special services (for example, installation of new equipment, after-hours support) well in advance of date required
- Be aware of and comply with the security standards, policies, and
- procedures established by the University of Illinois, as well as AITS policies for
- AITS provided services such as eMail and network
- Be available to provide critical information to assist in the resolution of cyber incidents
- Provide UA staff to support, advise and assist with departmental information security matters
- Assess, manage, and mitigate agency information security risk
- Define and implement appropriate UA internal security policies, standards and procedures
- Provide security training to departmental staff
- Define and implement UA internal information security incident plans and procedures and integrate with the University of Illinois cyber security incident plan
- Provide internal UA security incident response oversight
- Develop and follow UA level project plans to implement agency level security

How Do We Charge?

Currently, AITS does not charge for routine security services. Extensive and/or on-going security reviews may require funding negotiated on a case-by-case basis.

***Our Service Catalog is based on material that was developed by The State of North Carolina's Operational Excellence Program's Service Catalog and adapted with their permission. ***

DOCUMENT OWNER/APPROVAL

Service Catalog Owner: Ken Rowe

Concurrence:

Service Catalog Owner Date

Computer Operations Engineering Date

Approval:

Associate Vice President - AITS Date

REVISION CONTROL

Document title	Information Security Consulting and Support
Author	Ken Rowe
File reference	Information Security Consulting and Support

Date	By	Action	Pages
1-10-10	Ken Rowe	Initial Content	1-4

REVIEW/APPROVAL HISTORY

This service catalog shall be subject to a review on an annual basis.

Date	By	Action	Pages
4-23-12	Ken Rowe	No Revisions	
6- -10-13	Ken Rowe	Delete perform modified penetration testing (Pen Test) to determine full scope of vulnerabilities. Need to do this bullet point Also, deleted Secunia Corporate Software inspector bullet	1 and 2