



Information Security Training & Awareness

Online Training & Awareness Project Briefing Expectations & Responsibilities Information Security Manager's Forum, March 4, 2008 *Revised September 20, 2010*



Information Security Training & Awareness

(1) Why is awareness important?

- Obligation to protect private information belonging to our customers (students, faculty, staff)
- It promotes healthy behavior that can lessen the risk of disclosure, identity fraud and its potential costs
- Internal costs, external fines to address breaches can be enormous
- Protect the University from public embarrassment or jeopardize public trust
- Lead to more favorable audits from applicable authorities
- Do not want to jeopardize external funding sources (budgets, grants, alumni giving)



Information Security Training & Awareness

(2) What have we been doing for training & awareness

For technical people

- Information Security Managers Forum program
- Vulnerability alerts
- Technical classroom training
- Presentations to IT Steering & college executive teams
- Security executive management reporting (incidents, security project status)

For everyone

- Security Advisories
- security.cuny.edu, IT Security policies & procedures
- College security awareness programs

Information Security Training & Awareness



(3) How are we expanding the training & awareness program?

- Online security awareness program, Enterprise Training Solutions
- Online security technical training, Enterprise Training Solutions
- Campus executive briefings
- CUNY/CIS InfoSec security newsletter
- Poster and brochure development
- Security visibility on CUNY Portal (alerts, message of the week)
- Articles in CUNY publications
- Content to re-brand and distribute on Campus
- Collaborate on campus information security days
- Online awareness program for faculty, students, staff



Information Security Training & Awareness

(4) What are the major milestones in the ***online awareness program for faculty, students, staff?***

- Approved by IT Steering
- Procurement
- Finalize course requirements (mandatory, suggested)
 - Awareness – faculty, staff (mandatory)
 - Awareness – students (mandatory)
 - Technical training – faculty, staff (suggested)
- Rollout plan
- Content review
- User enrollment
- Campus execution
- Progress tracking and reporting
- Status reporting to IT Steering

Information Security Training & Awareness



(5) What can you expect from CUNY-CIS Info Sec?

- Procurement
- Vendor, Enterprise Training Solutions, single point of contact, contract compliance and relationship management
- Definition of project expectations, deliverables, outcomes
- Project plan and leadership
- Ownership of overall project execution with campus ownership, execution and collaboration
- Timely follow-up on questions, issues
- Regular project meetings and status reporting (project, use of program)
- Prepare and submit to CISO written Central Office departments implementation plan
- Execution of program within Central Office departments

Information Security Training & Awareness

(6) What do we expect from the Campuses?

- Campus ownership of program and collaboration with CUNY-CIS InfoSec
- Work with Enterprise Learning Solutions for successful Campus implementation
- Single point of contact on your Campus, InfoSec Manager
- Prepare and submit to CUNY-CIS InfoSec written Campus implementation plan
- Administration and execution of program on your Campus
- Regular reporting of program progress
- Attendance at project meetings (InfoSec Manager forum)

Information Security Training & Awareness



- (7) General Information Security Training & Awareness – What can our current security vendor partners do for us?
- Provide content
 - Provide delivery mechanisms – posters, handouts, brochures

Information Security Training & Awareness



(8) Material distributed

- Copy of proposal submitted to procurement
- Security ETI projects approved by IT Steering
- Technical course catalog that is part of agreement



Information Security Training & Awareness

(9) Phase I – Technical Training Rollout

- 200 licenses – (10 per campus) to be distributed – campus distributes at their discretion
- 5 certification tracks – CISSP, CompTIA+, Security+, Certified Ethical Hacker, Computer Forensics



Information Security Training & Awareness

(10) Phase II – Awareness Training

- Designed for all students, faculty, and staff – 30 minutes in length
- Campuses design their own roll outs based on schedules, individual needs