

INFORMATION SYSTEMS QUESTIONNAIRE (ISQ)

Interviewee/ Title:

Name of Audited Department:

Completed By/ Title:

Date:

- I. General Unit Background Information (if this questionnaire is being used in an IT unit survey)
 - A. Very brief summary of main unit activities:
 - B. Number of individual employees (people and FTE):
 1. Faculty:
 2. Staff:
 - C. Approximate annual total unit expenditures:
 - D. Unit IT Governance Overview
 1. Number of IT staff:
 2. IT manager name(s):
 3. Third-party contractor name(s):
 4. Number of different sub-nets:
 5. Names of different IT management sub-groups within the unit, and the sub-nets (IP range or name) that they manage:
 - E. Has the department had an IT review as part of a departmental audit within the past three years?
 1. Were any of the department's information systems included in PricewaterhouseCoopers' July 2005 review of campus data privacy and security? If so, please provide a copy of the unit's response to any findings.
- II. Population
 - A. *Computers*
 1. How many computers are in use as:
 - a) Desktop workstations?
 - b) Portable workstations (laptops, notebooks, PDAs)?
 - c) Servers (all kinds)?
 - (1) How many of the above are web servers?
 - (2) How are the servers (all kinds) physically and logically secured?
 - d) Combined or other uses?
 - B. *Other devices* (please tell us how many there are of each)
 1. Printers
 2. Hardware Firewalls
 3. Dial-in modems
 4. Routers (including wireless access points) other than those managed by CNS
 5. Other
 - C. *Applications other than routine office software* (give name and purpose)
 1. *Used internally only* (that is, computer programs that the unit or a unit-contracted vendor provides for use by the unit's employees only):

INFORMATION SYSTEMS QUESTIONNAIRE (ISQ)

- a) If there is e-business software, is the department working with the campus Cashier's office (Payment Services) to verify its compliance with the payment card industry (PCI) standards for credit card transaction processing?
 - (1) *[Non-compliance could lead to penalties being imposed if there is a breach. The credit card industry has developed security standards with which departments who accept credit card payments must comply, and the campus Payment Services unit (campus Cashier) is working with departments to help them comply. There is now available assistance for compliance from a vendor with whom Office of the President has contracted on behalf of the entire UC system. The vendor offers self-test questionnaires and scanning services. Departments that accept credit cards need to be working with Payment Services on achieving and maintaining compliance with the standards.]*
2. Used externally (that is, computer programs that the unit provides for users other than its own employees, although its own employees may be users as well):

III. Selected IT Policy Compliance Elements

A. Campus Information Technology Security Policy (CITSP)

1. Does the department securely maintain documentation that, in a consolidated and concise way, identifies all of its electronic information resources (computers, other networked devices, applications (other than the common office applications), and data, (including restricted data)?
2. Has the department gone through a process of assessing risk, with regard to its electronic information resources, and deciding what actions to take to mitigate such risk? If yes:
 - a) Have the results of this process been securely documented?
 - b) Do regular departmental operations include periodically re-performing this risk assessment?

B. Minimum Security Standards for Networked Devices

1. Who has the responsibility for ensuring compliance with this policy throughout the unit?
2. Does the unit have a securely maintained security plan document covering its restricted data (note: currently this is a provisional requirement)?

C. Departmental Security Contact Policy

1. Has the role of security contact been assigned to someone, and the contact information provided to SNS?

D. UC Berkeley Restricted Data Management (RDM) registry requirements (Deans and Directors Memo, 11/20/2006)

1. Has the department identified all devices (including copy machines) that contain restricted data (per the campus' [list](#) of data elements on the Data Stewardship Council's web site)?
 - a) Is this identification securely documented? If so, please securely provide a copy for review.
2. Has the department deleted all restricted data that is not needed?

INFORMATION SYSTEMS QUESTIONNAIRE (ISQ)

3. Has the department encrypted all restricted data that is on portable devices?
4. Has the department registered, in the Restricted Data Management (RDM) registry program tool, all of its devices that hold restricted data covered by SB1386, HIPAA, or FERPA (required)?
5. Has the department also registered computing devices with other types of restricted data (strongly encouraged)?

E. **Berkeley Campus Plan Implementing the UC Requirements for Protection of Computerized Personal Information** (note: most of these requirements, in so far as they relate to departments, are covered by other IT policies now—below is the main thing that’s not explicitly covered elsewhere)

1. Is current e-mail or postal contact information securely maintained for all individuals whose personally identifiable information (for example, names with social security numbers, driver’s license numbers, or financial account and password information) is being kept?

F. **Policy on High-Cost Information Technology Acquisition**

1. Is the department acquiring computer hardware or software, making agreements with IT consultants or professional IT service providers, or making off-campus IT services arrangements (such as business process outsourcing), with a cost of \$100,000 or more?
If so, has a pre-acquisition review by the campus Chief Information Officer been formally requested?

G. **Data Management Use, and Protection (DMUP)**

1. Has the department taken action to discuss, train, and develop local procedures as necessary to ensure that employees who handle data know their roles and act to implement best practices as described in this policy?
2. How does the department ensure that it is not storing restricted data on workstations, laptops, or portable computing and storage devices unless absolutely necessary?
3. If restricted data must be retained on such devices, is this done only on a temporary basis, and are protective measures, such as encryption, employed to safeguard the confidentiality or integrity of the data in the event of theft or loss of the equipment?
[Per policy, permanent copies of restricted data should never be stored for archival purposes on workstations or portable equipment.]

H. **System Development and Maintenance Standards** (a systemwide policy known as IS-10—applies if there were applications noted in section II.C above). If the unit is the proprietor of applications, other than common office productivity software, that it uses internally and/or provides for use by other campus units:

1. Does the unit follow a process as described in this policy when it develops, changes, or purchases this application software?
If not, what process does the unit follow?

IV. Systems-related Responsibilities

A. *Availability*--Who is responsible for making sure that the department’s computers, printers, etc., are consistently operational?

1. Is this a full-time responsibility?

B. *Oversight of Mass E-mailing*—Does the department offer what could be called “commercial products or services”? Note: this definition, as

INFORMATION SYSTEMS QUESTIONNAIRE (ISQ)

interpreted by UCOP, could include athletic events, cultural/arts performances, licensing opportunities, publications, and membership solicitations (e.g., for museums or recreations centers). But the definition does *not* include advertising or promoting “activity”, *nor* does it include providing information about the University’s undergraduate, graduate, or professional degree-granting programs.

1. If yes, does the department use e-mail to advertise the products or services?

a) If yes, who is responsible for ensuring compliance with applicable anti-spam laws? [There are legal requirements placed on those who advertise via e-mail.]

2. [UCOP has issued guidelines to follow in order to ensure compliance with federal anti-spam law. Basically, the [guidelines](#) say that if a department is advertising products or services via e-mail, the e-mail advertisements have to identify themselves as ads, enable recipients to “opt-out” of receiving further ads, and provide the sender’s valid physical address.]

C. Assurance of Properly Licensed Software--Who is responsible for ensuring that all of the acquired software on departmental computers is properly licensed? How do they go about fulfilling this responsibility? [Unlicensed software could be violating copyright laws and therefore may subject the user and organization to penalties.]

V. Other Systems-related Issues

A. Business Continuity--Has the department determined which of its information systems are critical to its operations? [In this context, “information system” refers to a set of computer hardware, programs, and data with a particular operational function, like “our accounts payable system” or “our online ticket sales system”, or, more generally, “the computers used by our administrative staff” or “the computers in our student computer lab”.] If so:

1. How is this determination documented?

2. What back-up mechanisms does the department have to ensure the continuing availability of these critical systems?

3. Does the department have a business resumption plan that addresses disaster-recoverability of these critical systems? If so:

a) Is the plan consistent with the campus’ business resumption goal, as stated on the Office of Business Resumption [website](#), of resuming the teaching of core classes and the performance of a substantial number of research projects within 30 days after any major disaster?

b) Please provide a copy of the plan for review purposes.

B. IT Purchasing

1. Systemwide Agreements--Is the department aware of system-wide purchasing agreements with regard to information technology?

a) [The campus has been advised of the following informational site by David Willson of Information Systems and Technology’s Strategic Technology Acquisition unit (via e-mail 10/7/2005): <http://www.ucop.edu/irc/tas/agreetoc.html>]

2. Unit-level Purchasing Process--Does the department’s purchasing process for networked devices include ensuring that an intended purchase will be compliant with the campus minimum security standards (if yes, explain how this is accomplished)?

INFORMATION SYSTEMS QUESTIONNAIRE (ISQ)

3. *Unit-produced RFP Language (RFP = Request For Proposal— formal request sent to potential vendors or posted for their access and response) --Where an RFP process is used to purchase networked devices, does the department take steps to ensure that compliance with campus minimum security standards is part of the requirements communicated to prospective vendors (if yes, explain how this is accomplished)?*
- C. *Vulnerability and Restricted Data Scanning--Would the system administrator be willing to have vulnerability and restricted data scans performed on the department's computers? [This enables preventive assessment of risk. Audit and Advisory Services, in collaboration with the department's system administrator, would scan devices on the department's network with tools made available to the campus by the campus System and Network Security office.]*
1. *Web server vulnerabilities—If the unit is operating web servers, have those servers been checked for PHP-related vulnerabilities and evidence of PHP-related compromise (per 9/4/2007 e-mail from SNS's John Ives)?*