September 7, 2012

Dear Colleagues:

As many of you are aware, as part of UCR’s policy relating to the safeguarding of personal protected data stored on UCR computer systems, the campus is required to complete an annual inventory of all electronic systems containing protected data. While this will mark the fifth consecutive year for the annual reporting, it is important to note that UCR is expanding the annual inventory to include not only protected data, but to include systems that contain sensitive data and or provide electronic services critical to campus operations. The addition of reporting on sensitive or essential data locations, is a requirement as a result of an internal audit report on Physical Security.

It is important to note, that the definition of personal protected information has been expanded to include Medical Information. Please see below.

In addition to reporting on this new data category, it is important to set the stage for further assessment of highly sensitive data locations. Therefore, you are being asked to rank the systems based on the following factors:

- The level of sensitivity of the Electronic Information Resource, and

- The level of criticality or overall importance of the Electronic Information Resources to the continuing operations of the campus or of the University.

The level should be assigned as follows: HIGH - very sensitive or critical OR contains Personal Protected Data, MEDIUM - relatively sensitive or critical, or LOW - minor sensitivity or criticality. To accomplish this, a summary sheet is provided which is to be completed at the Organization level.

Based on this inventory of systems, C&C will collaboratively engage with departmental / organizational leadership in a physical risk assessment of those systems deemed High level of sensitively or criticality or that contains Restricted and/or Limited data as defined by Information Business & Finance Bulletin IS-3.

For those systems at risk, C&C will collaboratively engage with departmental / organizational leadership in formulating a plan and budget to either remediate the existing physical space or to migrate the system in question to the off campus data center (Acorn Technology). Please note that space in UCR’s data center is very limited and the migration of systems to co-location space, even those deemed Essential and/or that contain Restricted and/or Limited data, is problematic. Nevertheless, this process will highlight for campus management the systems most at risk and the costs / opportunities associated with risk mitigation.

Please note that C&C will present a summary of its findings to campus leadership (e.g. Deans, Vice Chancellors, and the EVCP).
C&C would like to complete this inventory process by October 31, 2012.

Inventory Information:

As Responsible Administrative Officials or Data Proprietors, C&C is requesting that you please submit an inventory of systems (operated under your scope of responsibility) containing protected data. Many of you participated in last year's inventory process and can revise the forms submitted for last inventory, if applicable. If you have no systems with PPI, please simply send an email stating such.

For new submissions, attached please find a protected word form (please note that you may edit last year's form for systems reported last year, but a form must be re-submitted). A separate form should be used for each system inventoried. Upon completion of your Organization’s inventory, please provide a soft copy of your submittal. For large organizations it may be best to place your inventory on a protected flash drive, as opposed to emailing multiple word files.

In addition to providing the completed forms, please provide a summary listing of the systems (form attached), a description of the data, and the level of sensitivity and criticality.

C&C recognizes that the aforementioned process is time consuming and requires on-going review. Nonetheless, if security breaches occur, the effort to contact individuals and address concerns and questions can be overwhelming. Thus, our hope is that the time spent inventorying and managing systems containing protected data will help avoid the costly remediation efforts required when security breaches occur.

**Once again, C&C would like to complete this inventory process by October 31, 2012 at the latest.** If you have any questions or concerns, please give me a call.

The following web pages below provide additional information and resources pertaining to this issue:

List of Administrative Officials / Data Proprietors:

Resources on Security:
http://www.cnc.ucr.edu/security/

Policies and Procedures:

Updated Definition of "Personal Information"

The definition of "personal information" for this California requirement is an individual's first name or first initial and last name, in combination with any one or more of the following:

- social security number
The relevant California requirement defines medical information to mean any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; and health insurance information to mean an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. (excerpt from UCOP IS-3, page 23)

Sincerely,

Shelley Gupta
Chief Financial & Administrative Officer
Computing & Communications
University of California, Riverside
Phone: (951) 827-2877
Email: shelley.gupta@ucr.edu

1- The "account number" corresponds to an individual's financial account