Computer and Information Security Policy

OVERVIEW
This document describes the Computer and Information Security Policy used within the Department of Undergraduate Education. Staff are also responsible for adhering to campus and UC policies as defined in “Section 714-18: Computer and Network Use Policy” (http://www.policies.uci.edu/adm/pols/714-18.html).

CONFIDENTIALITY AND PROFESSIONALISM
DUE-IT staff has privileged access to all data stored on servers and machines they maintain; this level of access is required for the type of work they do. As part of their code of professional conduct, DUE-IT members agree that they will only access files when required for the performance of their work; any information viewed by DUE-IT staff will be protected and kept confidential.

DUE staff should not save personal, non-work related information on DUE systems. Incidental personal use of UCI electronic communications is permitted as described in “Section 800-15: UCI Guidelines for the University of California Electronic Communications Policy” (http://www.policies.uci.edu/adm/procs/800/800-15.html). Personal use of UCI computing and networking resources during non-University paid time is allowed with a supervisor’s permission; all users are still required to comply with “Section 714-18: Computer and Network Use Policy” as well as local unit policies when using University resources.

ACCOUNTS
All access to computer, computing resources, and electronic information is controlled by user accounts.

Types of accounts
There are three types of user accounts: staff accounts, student accounts, and group/shared accounts.

Staff accounts are given to individuals employed by DUE in staff or faculty positions. Student accounts are given to individuals employed by DUE in student positions. These accounts should be not shared with other users. The user of the account is responsible for how the account is used and following all applicable usage policies.

Group/Shared accounts can be requested for situations that require more than one person to have access to a resource that cannot be shared by individual accounts. The Group account must have a sponsor who maintains primary responsibility for how the account is used and for authorizing which individuals are given access to the account.
Creation
To create a Staff or Student account, the hiring manager must initiate an e-mail request to due.it@uci.edu; accounts will not be created before the employee’s start date. Requests for Group accounts must be approved by the head of the unit in consultation with DUE-IT. The hiring manager or responsible person should specify the account’s access rights within their unit’s shared folder. Access to another unit’s share folder must be approved by the director of the unit that owns the share folder.

Any account that has access to sensitive data, especially personal identity information (http://www.nacs.uci.edu/datasetsecurity/) must be registered with DUE-IT. The head of each unit or their designate should audit the access rights to sensitive data maintained by their unit annually to ensure that appropriate policies are followed and to evaluate if access to sensitive data is still required.

Termination
All Staff and Student accounts will be closed automatically when the user leaves DUE employment. The unit’s director must submit a request to DUE-IT for any extension of account access beyond a user’s termination date. Student accounts will be closed automatically at the end of each quarter unless renewed. Files owned by closed accounts will become the responsibility of the unit to maintain. In the case of electronic communications for a closed account, the “Access Without Consent” rules defined in “Section 800-15: UCI Guidelines for the University of California Electronic Communications Policy” (http://www.policies.uci.edu/adm/procs/800/800-15.html) will be followed.

CONTROLS
The following mechanisms are in place to protect the DUE computing environment:

Inventory
DUE-IT is responsible for tracking all DUE-owned computing equipment and software licenses; groups with their own IT support staff, specifically CTS, TLTC, and UROP, are exempt from this and are responsible for their own equipment and software. DUE-IT will install and maintain DUE-owned systems upon request and will provide assistance and consultation for all computer hardware and software purchases. To assist in the tracking of inventory, any user taking computing equipment home should notify DUE-IT in advance.

Off-Campus Access
All public access to DUE computing resources is governed by campus policy, and servers providing public information must be registered with NACS to permit access through the campus firewall. Direct access to internal departmental resources (e.g. sensitive data, desktop machines, etc.) is not permitted from off-campus unless using the UCI campus VPN, Secure Shell (SSH), and/or Secure FTP (SFTP) applications; DUE-IT will provide assistance with setting up and using these applications.

Patching
All desktop and laptop computers are configured for automatic patching. DUE-IT must be notified if an exception to this policy is required; the requestor then assumes responsibility for patching the system on a regular basis. DUE-IT will announce patches and maintenance
windows for department servers; most patching will be performed within 7 days of a
Microsoft patch release.

Non security-related application patching and updating on desktop and laptop machines
will be performed only by request. In the event of a security-related application update,
DUE-IT will contact the affected individuals and schedule a time to install the update.

Data Backups
Backups for the production DUE servers are performed using NACS’s Data Backup and
Recovery Service; the service maintains 2 months of previous backups. Users are strongly
advised to save/store work-related data on the provided network shares which will be
backed up regularly. All non-work-related data are the responsibility of the primary user
to backup. In the event of a catastrophic failure, DUE-IT will reimage the system with the
original image, if available.

Data Security Policy:

OVERVIEW:
This section describes the Data Security Policy used within the Department of
Undergraduate Education to ensure compliance with UCI’s commitment to protect the
privacy of student records and other sensitive data
(http://www.reg.uci.edu/privacy/full_privacy.html).

DEFINITIONS:
Sensitive Data, as used in this document, refers to any information that could compromise
the Division of Undergraduate Education or the individuals referenced by the data if such
data were obtained by someone who is not authorized to view such data.

Student Data, as used in this document, refers to information related to individual
identifiable students. Aggregate impersonal data (such as for statistical analysis) is not
included in this definition.

DATA ACCESS:
DUE maintains a number of repositories of student personal data. Access to this data
should follow the same "need to know" guidelines established by the Registrar and
Admissions Offices. When hiring staff or changing staff duties, department managers
should send e-mail to due.it@uci.edu to notify DUE-IT of the change. Department
managers should also require training and sign off for staff members who will be accessing
student data.

DATA RETENTION:
Each department, following guidelines established by the Registrar, should determine a
maximum period for retaining personal student data and establish periodic procedures for
expunging expired data. Department managers should consult with DUE-IT on establishing
methods and processes for deleting expired data.
DATA TRANSMISSION:
DUE-IT is primarily responsible for the electronic transmission of data sets between DUE and external campus units—especially the Registrar, the Office of Admissions and the Financial Aid Office. Requests for student data should be submitted to DUE-IT, preferably with at least two weeks advance notice. ARS is largely excluded from these requirements.

If, in exceptional cases, a DUE unit determines—ideally with DUE-IT consultation—that it is necessary to exchange data directly with an external unit, the following procedures should be followed: Electronic transmission of student personal data should be well documented. Ideally, any data transmitted electronically should be encrypted and performed through secure modes of transmission; examples of secure modes of transmission are secure websites like UCI’s Webfiles and secure applications like UCI’s VPN. The more personal and sensitive the information, the stronger the need is for documentation, secure processes, and encryption.

DATA REQUESTS:
Departments are encouraged to work with DUE-IT staff whenever they need to make an ad-hoc request for a large number of student records from external units (e.g. a hundred records or more), especially the Registrar, the Office of Admissions, or the Financial Aid Office.

DATA STORAGE AND TRANSPORTATION:
The copying of sensitive data to portable devices and media, such as laptops, USB keys, DVD-ROMS and portable hard drives should be severely limited, especially if said devices and media will be removed from DUE premises. If it is determined that copying and transporting such data is necessary, reasonable efforts should be made to encrypt the data and to physically and electronically secure the devices and media. Users should send e-mail to due.it@uci.edu to request assistance with encrypting sensitive data.

In addition, sensitive data should not be stored on local disks or removable media without explicit authorization from the unit’s director and notification to due.it@uci.edu. All instances of sensitive data must be recorded in the campus-wide Electronic Information Resource (EIR) database by DUE-IT. DUE-IT scans department machines periodically for restricted data.

DISPOSAL OF DATA STORAGE DEVICES:
DUE departments should consult with DUE-IT staff whenever disposing of a device (including desktop PCs) used to store student data or other sensitive information.

APPLICATION AND DATABASE DEVELOPMENT:
DUE Programming and Database staff should establish a set of best practices and guidelines for keeping code, web applications, and databases secure. Ideally, this would be followed by all developers in all DUE departments, and would be updated regularly to reflect technological innovations and changing security threats.