GENERAL ORDER

3

EFFECTIVE: 6 April 2009

REVISED: 1 January 2010
20 June 2011
18 December 2013

SUBJECT: Electronic Communications – Acceptable Use

ISSUED BY: Fernando Solorzano

I. PURPOSE

The purpose of this policy is to establish procedural guidelines for the use electronic communications systems, including activity involving the Internet and Police Data Network (PDN), individual workstations and mobile devices, and access to data stored in local, state, and federal computer systems. Electronic mail and faxes, which are transmitted over the Internet, PDN, wired or wireless telephone or data systems are subject to all provisions of this policy.

II. AUTHORIZED PERSONS

Access to computers, networks, and electronic communications on behalf of the Department is limited to employees, volunteers, authorized vendors, and contractors. Hereafter in the policy, authorized persons will be referred to as employee(s).

Unauthorized persons shall not be permitted to access or otherwise utilize computers or network equipment.

III. PERMISSIBLE USE

The use of any department computer resource is restricted to those activities related to department business. Use of computer and electronic communications by employees is authorized in support of the mission of the Department and the administrative functions that support that mission. Incidental personal use is only allowed as provided for in this order.

University Police Department employees and other authorized users shall adhere to this policy as well as guidelines set forth in the University's "Acceptable Use of CSULB Electronic Communications Systems and Services" and "Information

Security Policy". Should a conflict arise between Department and University policy, the more restrictive policy shall prevail.

Employees are expected to abide by the standards of conduct delineated in all other chapters and sections of the Departments Policy and Procedures Manual and General Orders as they may be applied to the use of electronic communications and the use and release of information.

Employees are expected to use electronic communications and network systems with a high degree of professional and personal courtesy. Employees must ensure that the tone and content of electronic communications are businesslike, exclude inflammatory remarks or inappropriate language, and do not improperly release confidential, sensitive, or legally protected information.

Employees may use electronic communications systems and services for incidental personal use provided that such use does not:

(a) Interfere with the Department or University's operation of electronic communications systems and services;
(b) Interfere with the employee's job performance or other obligations to the Department or University;
(c) Burden the University with noticeable incremental costs; or
(d) Create a security risk to the confidential or intellectual information maintained and protected by the Department or the University.

When noticeable incremental costs for personal use are incurred, users shall be responsible for reimbursement to the Department and/or the University as appropriate.

IV. PRIVACY

All data that is processed, stored, viewed, printed, or transmitted utilizing department resources is subject to review at any time, without notice to employees. This includes department email, workstations, laptops, servers, storage systems, removable media, department-issued telephones, smart phones, PDAs, pagers, or other mobile devices. Furthermore, all network traffic on the PDN is logged and subject to filtering and review.

Employees are cautioned that there is absolutely no right or expectation of privacy to be expected whenever Department resources are being used.

V. PASSWORDS

Department domain logon passwords must be sufficiently complex to insure the integrity of our security profile. Passwords must be at least 6 characters long and contain at least 3 of the following elements: upper case letters, lower case letters, number, and special characters. Passwords must be changed annually and must be

kept for at least 30 days unless compromised. Passwords must not be written down and may never be shared.

Employees with remote access tokens may not write down their PIN code and must advise the Information Management Bureau (IMB) immediately whenever a token is lost or stolen.

VI. STANDARDS AND OPERATIONS

The IMB is responsible for selecting and purchasing the standard desktop software suite for all departmental computers and for the administration of the software on all computers connected to the PDN.

All employees shall use the department's selected desktop software unless critical functionality is not available through the application. Specialized software needs will be assessed on an individual basis and, not withstanding technical conflicts, installed upon the approval from IMB and the Division Commander.

(a) INSTALLING LICENSED SOFTWARE**:**
Employees are prohibited from installing or maintaining unlicensed software on any department computer. Employees who wish to install licensed software on a department computer must have authorization form IMB and their Division Commander. The software installation and record of the installation will be the responsibility of IMB and a copy of the software license must be provided to IMB prior to the installation.

(b) LOGGING OFF:
To enhance security and ensure that shared computers are available to all employees, users shall logoff their computer when away from their workstation and at the end of the work shift,

All computers connected to the PDN must remain "on" at all times in order to provide after-hours maintenance.

(c) PROHIBITED DEVICES:
All dial-up connections, modem connections, or any other electron communication devices (wireless or otherwise) are prohibited on the PDN. Stand-alone machines not connected to the PDN may have dial-up or other connections with approval from IMB and the Division Commander.

IMB will ensure that all requests for any of the above connections are reviewed by knowledgeable staff. The purpose of the review will be to evaluate the risk and potential for illegal access to departmental systems, stored records, and confidential information. These findings will be reported to the requesting Division Commander so that an informed decision can be made.

(d) PROHIBITED USE

At no time during a response to a call for service will any employee of this department on or off-duty make any posting or send any message or notification to any social networking site, listserve or texting resource/outlet that comments in any way upon that departmental response unless directed to do so by a commanding officer and as part of a tactical response to that call for service.

(e) **EMAIL**

(1) USE

All employees shall check their campus email daily, while on-duty. Employees may access their campus email while off-duty; however, no employee will be required to do so.

(2) PRIVACY

All email messages transmitted over the PDN or campus network, or using campus server(s) are considered Department records and, therefore, are the property of the Department. The Department reserves the right to access, audit, and disclose for whatever reason, without notice to employees, any or all messages transmitted utilizing the system or any of its component parts.

The email system is not a confidential system. Therefore, it is not appropriate for confidential communications. If a communication must be private, an alternative method of communication should be employed. Employees have no expectation of privacy concerning communications in this system.

(3) PROHIBITED USE

Sending or forwarding of derogatory, libelous, defamatory, obscene, disrespectful, offensive, racist, sexually suggestive, and harassing or any other inappropriate messages on the email system is prohibited and will not be tolerated.

It is a violation of this order to transmit a message under another user's name or to forge an email message. Users are strongly encouraged to log off the network when their computer is unattended and are prohibited from sharing passwords.

(4) PERSONAL USE

Although the email system is meant for business use, the Department allows the reasonable use of email for personal use under the following guidelines:

a. Personal use of email should not interfere with work
b. Personal emails must also adhere to the guidelines in this order.

c. The forwarding of chain letters, junk mail, and executables is strictly forbidden
d. Do not send mass mailings
e. All messages distributed via the campus email system, even personal emails, are property of the Department and the University.

(f) TEXT MESSAGING

(1) USE

The purpose of this order is also to establish guidelines for the proper use and application of text messaging by employees of this department. This order refers to all department-issued electronic communication devices and includes all mobile phones, PDA's, pagers, and any other such wireless two-way communication devices.

Text messaging is a tool available to some employees as a means to enhance efficiency in the performance of job duties and is to be used in accordance with generally accepted business practices and current law. Messages transmitted on a text messaging system must only be those that involve official business activities or contain information essential to employees for the accomplishment of business-related tasks and/or communication directly related to the business, administration, or practices of the department.

(2) PRIVACY

All text messages transmitted on equipment issued by the Department are considered Department records and, therefore, are property of the Department. The Department reserves the right to access, audit, monitor, and disclose, for whatever reason, without notice to employees, all messages, including text transmitted on Department equipment. Text messages are not appropriate for personal communications. Three is no expectation of privacy in the use of Department-issued equipment.

(3) PROHIBITED USE

Sending or forwarding derogatory, defamatory, obscene, disrespectful, offensive, racist, sexually suggestive, and harassing or any other inappropriate messages via text message is prohibited and will not be tolerated.

(g) SOCIAL NETWORKING

(1) USE OF DEPARTMENT LOGOS AND IMAGES
Department personnel are prohibited from using Department logos, images, insignias, and emblems in conjunction with posting on social networking sites.

(2) IDENTIFICATION AS A DEPARTMENT MEMBER
Where it is evident that the poster is a member of the Department any ideas or opinions expressed must be clearly identified as being those of the poster and not reflecting those of the Department.

(3) RELEASE OF CONFIDENTIAL INFORMATION
Employees are expressly prohibited from releasing any confidential information related to the Department or the course of their employment on any social networking sites.

(h) REMOVEABLE STORAGE MEDIA

(1) USE
Removable storage media devices (i.e. “memory sticks”, or “thumb drives”) may be used to store and transfer files and documents subject to the following restrictions:

a. Files or documents that contain “Level 1 Confidential” data as per the University’s Records Management Standard or information that has been obtained via the CLETS network MUST be stored on department-issued encrypted devices.

b. Removable storage media devices may not be used to install unauthorized applications on department assets.

c. Removable storage media devices may not bypass antivirus software.

d. Files or documents that are subject to copyright protection may not be stored on removable storage media devices unless proper permission has been obtained or “fair-use” statute applies.

(2) PRIVACY
All data that is processed, stored, viewed, printed, or transmitted utilizing department resources is subject to review at any time, without notice to employees. This includes any files that may be contained on a personally owned removable storage device that is accessed from a department-owned system.

(3) PROHIBITED USE
Level 1 Confidential and CLETS-provided information may not be stored on any device except for department-owned encrypted devices specifically issued for that purpose.

(4) PERSONAL USE
Incidental personal use of both personally-owned and department-owned devices is permitted, subject to the operational and privacy restrictions described in this section.

APPROVED