International American University

Introduction

This document provides guidelines for appropriate use of computer facilities and services by students, faculty and staff at International American University (IAU) and its offices across the world. It is not a comprehensive Document covering all aspects of computer use. It offers principles to help guide members of the International American University community, and specific policy statements that serve as reference points. It will be modified as new questions and situations arise.

Information technology is a rich resource for innovation in the furtherance of IAU's academic mission. They increase the risks of actions, deliberate or not, that are harmful in various ways, including: (a) interference with the rights of others; (b) violation of the law; (c) interference with the mission of the University; or (d) endangering the integrity of the University's information computer network.

- The guidelines therefore call for respectful and responsible use of the computer networks and the users within the community must understand the perils of illegal use, exchange, or display of copyrighted, deceptive, defamatory, or obscene materials on a web page or through other electronic communication channels.
- When individuals misrepresent either themselves or the University, or when they act by computer in a manner unacceptable within the University or in the larger community, the integrity and mission of the University itself is endangered.
- Finally, the guidelines seek to protect the integrity of the University information systems themselves: the computing or networking resources need to be accessible and secure for appropriate uses consistent with the mission of the University; the usurpation of these resources for personal gain, commercial gain or without authorization is unacceptable.

Policy Statement

The use of International American University's (IAU) automation systems, including computers, fax machines, and all forms of Internet/Intranet access, is for IAU business and for authorized purposes only.

- Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to IAU.
- Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to IAU's business; distract, intimidate, or harass co-workers or third parties; or disrupt the workplace.

Use of IAU computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

1. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate IAU purposes;
2. Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
3. Misrepresenting oneself or IAU;

4. Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
5. Engaging in unlawful or malicious activities;
6. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either IAU's networks or systems or those of any other individual or entity;
7. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
8. Sending, receiving, or accessing pornographic materials;
9. Becoming involved in partisan politics;
10. Causing congestion, disruption, disablement, alteration, or impairment of IAU networks or systems;
11. Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", watching of movies/shows, or private/personal/instant messaging;
12. Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
13. Using recreational games; and/or
14. Defeating or attempting to defeat security restrictions on IAU systems and applications.

IAU will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of IAU's automation systems is expressly forbidden.

Use of IAU resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files

IAU owns the rights to all data and files in any computer, network, or other information system used in IAU.

IAU also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content.

Employees must be aware that the electronic mail messages sent and received using IAU equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by IAU officials at all times.

IAU has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with policy and state and federal laws.

No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate IAU official.

The University has a right to expect that computer users will properly identify themselves. Computer accounts are assigned and identified to individuals. Don't misrepresent yourself.

Avoid excessive use of computer resources. They are finite and others deserve their share. "Spamming" and similar inappropriate uses of University resources are not acceptable. Web pages that are accessed to an excessive degree can be a drain on computer resources and, except where significant to the University's mission, may require the University to ask that they be moved to a private Internet provider.

IAU has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software.

Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and IAU (IAU) rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of IAU policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others.

Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Intranet Browser(s)

The Internet is to be used to further IAU's mission, to provide effective service of the highest quality to IAU's customers and staff, and to support other direct job-related purposes.

Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are IAU resources and are provided as business tools to employees who may use them for research, professional development, and work-related Communications.

Limited personal use of Internet resources during lunch break or employee's personal time is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating IAU security policy, copyright, and licensing agreements.

All IAU policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, IAU information dissemination, standards of conduct, misuse of IAU resources, anti-harassment, and information and data security.

Personal Electronic Equipment

IAU prohibits the use in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of image-recording device without the express permission of IAU and of each person whose image is recorded.

Employees should not bring personal computers to the workplace or connect them to IAU electronic systems unless expressly permitted to do so by IAU.

Any employee bringing a personal computing device or image recording device onto IAU premises thereby gives permission to IAU to inspect the personal computer or image recording device at any time with personnel of IAU's choosing and to analyze any files, other data, or data storage media that may be within or connectable to the personal computer or image recording device in question.

Employees who do not wish such inspections to be done on their personal computers or imaging devices should not bring such items to work at all.

Implementation

A. All University codes of conduct apply to information technology as well as to other forms of communication and activity.
B. Systems managers or other individuals within an academic or administrative unit may be empowered to suspend some or all privileges associated with computer use in cases of misuse or threat to the integrity of all or part of the University's information management resources.
C. Complaints or concerns about another's use of University computer resources should be directed to the administrator responsible for the facility or resource in question.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment. In addition, the employee may face both civil and criminal liability from IAU or from individuals whose rights are harmed by the violation.

IAU IT POLICY ACKNOWLEDGEMENT OF RECEIPT

I acknowledge that I have received a copy of the IAU IT Policy. I understand the contents of this policy and will act in accordance with these policies and procedures while I am associated with IAU.

____
Name (Please Print)

____
Signature

____
Date