Process Number: BP-03-016
Approved By: James August
AVP for Information Technology Services

Effective Date: 04/10/2024

Acceptable Use Policy of IT Resources

PURPOSE:

The purpose of this policy is to outline the acceptable use of IT Resources at CSUCI. These rules are in place to protect the employee and CSUCI. Inappropriate use exposes the University to cyber risks, including virus attacks, ransomware, compromise of network systems and services, data breach, and legal issues.

BACKGROUND:

The Acceptable Use Policy is not to impose restrictions contrary to CSUCI's established culture of openness, trust, and integrity. The university is committed to protecting CSUCI's employees, students, and the University from illegal or damaging actions by individuals, knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and sFTP, are the property of CSUCI. These systems are to be used for business purposes that serve the interests of the University. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

BUSINESS PRACTICE:

Applicability:

1.1.1 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of University information.

1.1.2 You may access, use, or share University information only to the extent it is authorized and necessary to fulfill your assigned job duties.

1.1.3 Employees are responsible for exercising good judgment regarding the reasonableness of use of Information Technology resources.

1.1.4 For security and network maintenance purposes, authorized individuals within CSUCI may monitor equipment, systems, and network traffic at any time.

1.1.5 ITS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.2 Security and Proprietary Information

1.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

1.2.2 System-level and user-level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

1.2.3 All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 20 minutes or less. You must lock the screen or log off when the device is unattended.

1.2.4 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

1.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the university authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CI owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

1.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CSUCI.
2. The use of non-CSUCI computers for official university work. Employees must use CSUCI-provided equipment in order to meet compliance with business practices and policies.
3. The installation of any copyrighted software for which CSUCI or the end user does not have an active license is strictly prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).
6. Revealing your account password/passphrase to others or allowing others to use your account. This includes family and other household members when work is being done at home.
7. Using a University computing asset to actively procure or transmit material that violates sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any University account.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Introducing honeypots, honeynets, or similar technology on the University network.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Using VPN internally to avoid CSU security control and processes. Bypass vendor restrictions by changing locations based on VPNs for unauthorized reasons.

1.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within CSUCI's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CSUCI or connected via CSUCI's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2. Policy Compliance

2.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

2.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions:

- Blogging is the activity of writing and publishing online posts on a website or platform, usually on a specific topic or niche.
- Proprietary information is any information that belongs to a person, company, or organization and is not publicly available or shared. It may include trade secrets, patents, copyrights, customer data, business plans, or other confidential or valuable information.
- Spam is any unsolicited or unwanted electronic message, usually sent in bulk to multiple recipients, often for advertising, phishing, or malicious purposes.
- Ransomware is a type of malware that encrypts the files or data of a victim and demands a ransom for their decryption. It may also threaten to delete or expose the data if the ransom is not paid.

Assessment Requirements

Assessment requirements and history are listed in the grid below.

Description	Frequency	Role Assigned	Date Completed
General review of this business practice	Annual	CIO	04/10/2024

Revision History

BP Nbr:	BP-03-012	Enacted Date:			
Revision Nbr:	001	Revision Date:	04/17/2024	Revised By:	C Miranda