TABLE OF CONTENTS

Contents

office, the registrar's office, financial aid, admissions, enrollment, marketing, student affairs, advancement, industry leadership, human resources, information technology, planning and strategy, finance, restaurant operations, accreditation, or branch campus and international operations.

Confidential Information – Confidential Information is any non-public knowledge, documentation or information that belongs to the CIA, as well as any data protected by federal and/or state law against unauthorized use, disclosure, modification or destruction. This Confidential Information any may include but is not limited to business plans, strategy plans, curriculum, trade secrets, proprietary information, marketing plans, strategies and data, admissions information, student records, medical information, financial data, employment records, research data, advancement data and information security data.

Mobile Communication Device (MCD) – A communication device that is portable and designed to be carried by an employee of the CIA to carry out CIA business communication activities. Mobile communication devices include, but are not limited to cell phones, smart phones, Blackberry units, iPhones, iPads, Droids, and hands-free devices.

Personally Identifiable Information – Personally Identifiable Information (PII) is any information that uniquely identifies an individual, and which may be used to identify, locate or contact an individual. Common examples of PII are individual names, phone numbers, addresses, grades, social security numbers, employee numbers, student numbers, and dates of birth.

Resources – Resources are CIA's computer network, servers, personal computers, laptops, handheld computers, PDAs, telephones, smartphones, voicemail, mobile devices, etc.

D. PROCEDURES

AUTHORIZED USE

An Authorized User is any person who has been granted authority by the CIA to access its computing and network systems and whose usage complies both with the level of access granted and also with this policy.

The Department which "owns" the data contained within any given computer software application shall be responsible for authorizing use of or access to said application or the

associated data contained therein. This shall apply to all applications which are either hosted directly by the CIA or provided through outsourced, third party providers. For the purposes of this policy both shall be considered CIA network or computer resources. Unauthorized use is strictly prohibited. The terms "Authorized User" and "user" are hereinafter used interchangeably.

PRIVACY

Any information traffic sent over the CIA's network and computing resources, whether wire or wireless, becomes CIA property. Users cannot have any expectation of privacy concerning this information, its source, or its destination. At all times, CIA has the right, but not the obligation, to access, monitor, and record network and computer system usage. There are systems currently in place to record such usage, as well as the files, information, and location of all sites accessed by users. Although limited personal use that does not violate any CIA policy or otherwise interfere with job duties is not prohibited in all cases, users should not expect that such use entitles them to any expectation of privacy in anything that they access, view, create, store, send or receive on or through the network or computer system, including any personal messages, even personal messages sent or received from personal email accounts, including without limitation web-based email accounts, such as Yahoo and Google email accounts.

Use of passwords to gain access to any CIA computing or network resources does not mean that users should have any expectation of privacy in the material that they access, view, create, transmit, store or receive via or on The CIA computing or network resources. The CIA has the ability to permit IT and other personnel access to all activity on the computing and network system, including without limitation all information and materials accessed, viewed, created, **stored on or transmitted through its computing and network sy**

10. **Disrupting or damaging the academic, research, administrative, or related pursuits of another;**
11.

I. Unauthorized Activities

Users are prohibited from attempting to circumvent or subvert any security measures implemented for the CIA computing and network systems. The use of any computer program or device to intercept or decode passwords or similar access control information is prohibited. This section does not prohibit use of security tools by IT system administration personnel, in a manner consistent with CIA policies and procedures.

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized users of access to or use of such resources are prohibited.

J. Denial of Service Attacks

Denial of service attacks, 'fire bombing', 'flaming', 'hacking', 'spoofing', 'cracking', and any other type of malicious or mischievous intrusion or network attack against any network and computing resource user, any host on the CIA Network, or any other host on the Internet by a any member of the CIA community will be grounds for immediate removal of said individual and devices from the CIA network.

K. Harmful Activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software, or data belonging to the CIA and the like.

L. Unauthorized Access

All users are also strictly prohibited from:

1. **Damaging computer systems;**
2. **Obtaining extra resources without authority;**
3. **Depriving another user of authorized resources;**
4. **Sending excessive messages or sending frivolous information, documents or messages such as chain letters or jokes;**
5. **Gaining unauthorized access to CIA computing and networking systems;**
6. **Using a password without authority;**
7. **Utilizing potential loopholes in the CIA computer security systems without authority;**
8. **Using another user's password; and**
9. **Accessing abilities used during a previous position at The CIA.**

M. Tampering of Equipment or Resources

No computer equipment, including peripherals, telephones, networking resources or software applications will be moved from its current location without authorization from IT. This includes the tampering, modification, or additions to network software, hardware, or wiring.

N. Use of Licensed Software / Downloading

No software may be installed, copied, or used on CIA resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

Only authorized personnel may install legal software on CIA-owned resources. The downloading of software via the Internet is prohibited due to the possibility of legal or copyright ramifications.

O. Personal Business, Political Campaigning, And Commercial Advertising

The CIA's computing and network systems are a CIA-owned resource and business tool to be used only by authorized persons for CIA business and academic purposes. Except as may be authorized by The CIA, users should not use The CIA's computing facilities, services, and networks for:

1. **Compensated outside work;**
2. **The benefit of organizations not related to The CIA, except in connection with scholarly**

ned we susers eted oom b01107(o)7.01294391(o)-2.00301001(9-4..01009(T)6.98649(d)-4.00391(i)-1(n)-3

B. CIA Access

The CIA may access usage data, such as network session connection times and end-points, CPU and disk utilization, security audit trails, network loading, etc. Such activity may be performed within the reasonable discretion of IT management, subject to CIA approval.

C. Availability

IT will make every effort to insure the operation of the CIA network and the integrity of the data it contains. In order to perform needed repairs or system upgrades, IT may, from time to time, limit network access and/or computing resources for regular or unexpected system maintenance. IT will make every effort to give notice of these times in advance, but makes no guarantees.

D. Departmental Responsibilities

Each CIA department has the responsibility of:

1. **Supporting the enforcement of this policy;**
2. **Providing for security in such department areas;**
3. **Encouraging users to save all files to a network drive (network drives are backed up every day where local drives are not and external media tend to be less reliable); and**
4. **Notification of personnel changes.**

E. Wireless Access Points

The Information Technology department provides wireless service for use by CIA faculty,
A y,

All users and departmental units have the responsibility to report any discovered unauthorized access attempts or other improper usage of CIA computers, networks, or other information processing equipment. If a security or abuse problem with any CIA computer or network facility is observed by or reported to a user, such user shall immediately report the same to such user's department head, Human Resources and/or the Associate Vice President of IT.

B. Range of Disciplinary Sanctions

Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer or network access privileges, and disciplinary action, up to and including termination of employment. Some violations may constitute criminal offenses, as defined by local, state, and federal laws and the CIA may prosecute any such violations to the full extent of the law.

AMENDMENTS

The CIA reserves the right to amend or revise the policies herein as needed. Users will be provided with copies of these amendments whenever possible.

E. RESPONSIBLE CABINET MEMBER

Vice President - Administration & Shared Services: Designates individuals that have the responsibility and authority for information technology resources who will then:

a) Establish and disseminate enforceable rules regarding access to and acceptable use of information technology resources.
b) Establish reasonable security policies and measures to protect data and systems.
c) Monitor and manage system resource usage.
d) Investigate problems and alleged violations of this policy.
e) Refer violations to appropriate offices.

F. RELATED INFORMATION

CIA Harassment Free Campus Policy
CIA Social Networking Policy
Digital Millennium Copyright Act, as amended
Higher Education Act, as amended
Family Educational Rights and Privacy Act of 1974 (FERPA), as amended

California Education Code, as amended
Individuals With Disabilities Education Act, as amended
Federal Trade Commission Act, as amended
CIA Written Information Security Policy

G. POLICY HISTORY

Policy Editorial Committee & Responsible Cabinet Member Approval to Proceed: 10/10/18

_____

Policy Advisory Committee (PAG) Approval to Proceed: 10/10/18

_____

Board Approval to Proceed (if required), Date

_____

Cabinet Approval to Proceed: 12/3/2018

_____ _____

Policy Revision Dates:

_____

Scheduled Review Date: