Computer and Network Usage Policy

POLICY INFORMATION

Policy#: TECH-001

Original Issue Date: 7/23/2008

Current Revision Date: 4/7/2022

Initial Adoption Date: 7/23/2008

(Select a Policy Type)
☐ Organization Policy
☐ Legal Policy
☐ Education Policy
☐ Marketing Policy
☐ Finance Policy
☑ Technology Policy
☐ Compliance Policy
☐ HR Policy
☐ Enrollment Policy
☐ Advancement Policy
☐ Operations Policy

SCOPE

RESPONSIBLE OFFICE**Title**	**Department**
Vice President – Chief of Staff & Information Technology	Information Technology Services

Constituency	**Campus Locations**
(Select all that apply)	(Select all that apply)
☑ Staff	☑ Hyde Park
☑ Faculty	☑ Greystone
☑ Students	☑ San Antonio
☑ Contractors	☑ Singapore
☑ Visitors	

TABLE OF CONTENTS:

Contents

A. PURPOSE

The purpose of this Policy is to establish appropriate expectations, rules, and responsibilities for the proper use and management of all computing and network resources operated by The Culinary Institute of America (CIA). This Policy pertains to all CIA campuses regardless of the networks or systems used.

B. POLICY STATEMENT

The Culinary Institute of America's (CIA's) network and computing resources are shared resources, the use of which is a privilege and not a right. The primary purpose of these resources is to allow access to information that will support the CIA's mission. Thus, any actions that will inhibit or interfere with the use of the network is not permitted.

The use of the CIA's network and computer systems by any party should always be legal, ethical, and consistent with the CIA's mission. The CIA grants access to its networks and computer systems subject to responsibilities and obligations outlined in the Computer and Network Usage Policy and subject to all local, state, and federal laws.

Should it be determined that there has been a compromise or abuse to the CIA's network or computer resources from any CIA-issued user account or device, the CIA reserves the right to terminate that user's access and devices without notice immediately.

All Authorized Users are expected to cooperate with the requirements of the CIA's Information Privacy and Security Program, which employs administrative, technical, and physical safeguards.

C. DEFINITIONS

Authorized User – 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 with the level of access granted and with this policy.

College Activities – College Activities are any actions or initiatives conducted by the CIA related to running and staffing an institution of higher learning. Examples include, but are not limited to: activities related to educational curriculum and delivery, Student Financial and Registration Services, admissions, enrollment, career services, academic advising, 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. Confidential Information 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 portable wireless electronic device used for CIA business communication activities devices include but are not limited to cell phones, smartphones, iPhones, iPads, Droids, and other hands-free devices.

Multi-Factor Authentication (MFA) - An authentication system that requires more than one distinct authentication factor for granting access. The three authentication factors are something you know, something you have, and something you are. A user is granted access only after successfully presenting two or more separate and unique factors of authentication when logging into or accessing a computer or software application.

Personally Identifiable Information – Personally Identifiable Information (PII) is any information that uniquely identifies an individual and may be used to identify, locate or contact an individual either by direct or indirect means. Personal identifying information means the following:

- Social security number;
- Personal identification number;
- Password;
- Passcode;
- State or government-issued driver's license or identification card number;
- Passport number;
- Biometric data;
- Employer, student, or military identification number; or
- Financial account number, credit card number, debit card number, or any instrument or device that can be used to obtain cash, goods, property, or services, or to make financial payments, including without limitation payment cards and account numbers, in combination with any required security code, access code, or password such as expiration date or mother's maiden name that could permit access to an individual's financial account.

ITS Resources – Resources include the CIA's computer network, servers, computers, laptops, handheld computers, telephones, smartphones, voicemail, mobile devices, wireless routers, 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 given 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 a said application or the associated data contained therein. Authorized Use shall apply to all applications either hosted directly by the CIA or provided through outsourced, third-party providers. For 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 and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means.

Any information traffic sent over the CIA’s network and computing resources will become CIA property, whether wired or wireless. Users cannot have any expectation of privacy concerning this information, its source, or its destination. Any individual whose personal files are transmitted or stored on CIA resources shall have no expectation of privacy with respect to those files. At all times, the 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 and 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 Outlook, Yahoo, and Google email accounts.

The 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 they access, view, create, transmit, store or receive via or on The CIA computing or network resources. The CIA can permit ITS 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 system regardless of whether the information or material has been authorized with a user's password. Further, data may be electronically recalled or recreated irrespective of whether it may have been ''deleted'' or ''erased'' by a User. Because The CIA backs-up files and messages, and because of how computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased.

The CIA has the ability and reserves the right to investigate any and all activity on or through the computer and network systems, including without limitation any investigation of

information or data composed, transmitted, or received on the system, consistent with State and Federal law, including, but not limited to, monitoring internet browsing and personal email. Generally, any such access will be made only by those CIA representatives who need to know for legitimate business reasons or when necessary to protect a property right or other legal interest of the CIA.

Any personal, password-protected, internet-based email account, e.g., Gmail, iCloud, Outlook, Yahoo, etc. ("Personal E-Mail Account") may be monitored by the CIA under this Policy if CIA computer or network systems are used to access such account. For example, emails that are sent from, received or stored in a Personal Email Account may remain on CIA's computing or network resources (e.g., the hard drive on the computer assigned to you by CIA) and may be forensically retrieved and monitored by the CIA.

INDIVIDUAL RESPONSIBILITIES

A. Common Courtesy and Respect for Rights of Others

All users are responsible for respecting and valuing the privacy of others, acting ethically, and complying with all legal restrictions regarding the use of electronic data. All users are also responsible for recognizing and honoring the intellectual property rights of others. No user under any circumstances may use CIA computers or networks to engage in any activity prohibited under or within the College's Harassment-Free Workplace Policy, CIA Employee Code of Conduct, Social Network Policy, Violence in the Workplace Policy, Rules of Employee Conduct Policy, the CIA Employee Handbook. In addition, no user under any circumstances may use CIA computers or networks to transmit data or information that violates FERPA law. Some examples of this improper use of CIA computers or networks are:

1. Posting or transmitting expressions of hostility or bias against individuals or groups;
2. Posting or transmitting of offensive material such as obscenities, vulgarity or profanity;
3. Posting or sending inappropriate jokes or other non-businesslike material;
4. Posting, transmitting or viewing sexually explicit material;
5. Posting or messaging libelous or slanderous materials or remarks;
6. Name-calling
7. Harassing, terrifying, intimidating, or threatening another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family;
8. Contacting another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

9. Contacting another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection);
10. Disrupting or damaging the academic, research, administrative, or related pursuits of another;
11. Invading the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another, except as allowed for under FERPA law.

Users who engage in the conduct described above will be subject to disciplinary action, up to and including loss of computer or network access, expulsion, and/or termination of employment.

B. Content

Users who make use of forums, blogs, wikis, chat rooms, or social networking sites do so voluntarily, with the understanding that they may encounter material they deem offensive. Neither the CIA nor ITS assumes any responsibility for material viewed on these network communication utilities. Furthermore, ITS reserves the right to limit access to any content deemed offensive or lacking in educational value.

To ensure security and prevent the spread of viruses, users accessing the Internet through our network and computing resources must do so through the CIA Internet firewall.

C. Copyright Infringement & Peer-To-Peer File Sharing

The CIA respects the rights of copyright holders, their agents, and representatives and strives to protect those rights through compliance with copyright law prohibiting the reproduction, distribution, public display, or public performance of copyrighted materials over the Internet without permission of the copyright holder, except in accordance with fair use or other applicable exceptions. The CIA also respects the legal and appropriate use by individuals of copyrighted materials on the Internet, including but not limited to ownership, license or permission, and fair use under the United States Copyright Act.

Employees and students are responsible for understanding and complying with the rights of copyright owners in their use of copyrighted materials. Information can be found at the United States Copyright Office.

Unauthorized peer-to-peer file sharing on the CIA networks is prohibited and blocked by bandwidth-shaping technology. Violations of copyright law or this policy, including the use of technology to circumvent the blocking of peer-to-peer file sharing, may subject employees and students to disciplinary action, including but not limited to termination of network privileges, as well as civil and criminal liabilities. Further details and a summary of penalties for copyright law violation may be found in the CIA's Digital Millennium and Copyright Act Policy.

D. Responsible Use

All users are responsible for refraining from all acts that waste CIA computer or network resources or prevent others from using them. Each user is responsible for the security and integrity of information stored on both their CIA-issued and personal computer(s), voice mailbox, MCD, or any other portable device. Computer accounts, passwords, authentication codes, and other types of authorization are assigned to individual users and must not be shared with or used by others. All users must maintain the confidentiality of student information in compliance with all required states and regulations (including but not limited to the Family Educational Rights and Privacy Act of 1974, the California Education Code as interpreted in The Culinary Institute of America Student Records Policy, the Individuals With Disabilities Education Act, etc.).

E. Confidential Data and Personal Computer Security

To protect the CIA's private data, the CIA's private data must be stored on CIA-owned computers or within sanctioned and approved CIA approved applications. **Personally identifiable information** and other confidential information related to College activities must not be stored on individual faculty or staff personal computers, mobile devices, or other personally owned electronic devices including portable hard drives, Cloud storage, USB devices, cell phones, or any other device that has storage capabilities. In addition, no personal storage device should be connected to the CIA Administrative network or administrative devices, including PC, workstations, laptops, servers, or other hardware.

Personally identifiable information and other confidential information must be stored in and communicated in a password protected – encrypted file. No **personally identifiable information** and other confidential information should be openly communicated via email or shared openly to others.

When working remotely from the CIA campuses, Employees must use the CIA's Virtual Private Network (VPN) on a CIA-issued device to access CIA shared files and services. All CIA users must

have Multi-Factor Authentication enabled and configured to access CIA resources when working or accessing CIA resources off-campus.

Employees may use their devices such as laptops, home computers, mobile devices, smartphones, etc., to use the CIA's Office 365 applications. At no time should any documents, files, or other CIA data be saved or stored on a personal device.

F. Permitting Unauthorized Access

All users are prohibited from running or otherwise configuring software or hardware that would allow access by unauthorized users. These include, but are not limited to: remote desktop software, terminal services, Chrome remote desktop, and personal VPN tunnels.

H. Termination of Access

When a user ceases being a member of the CIA community or is assigned a new position and/or responsibilities at the CIA, such user shall not use facilities, accounts, access codes, privileges, or information for which they are not authorized in their new position. Upon termination, if the user has saved any CIA-owned information on any personal computing devices, these documents must be permanently deleted by the individual immediately to the satisfaction of the College.

I. Unauthorized Activities

Users are prohibited from circumventing or subverting any security measures implemented for the CIA computing and network systems. The use of any computer program or device to hide or obfuscate their identity, intercept or decode unauthorized data, or bypass access controls to information systems is prohibited. This section does not prohibit the use of security tools by ITS system administration personnel to conduct forensic auditing 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 and Phishing Attacks

Denial of service attacks, 'fire bombing', 'flaming', 'hacking', 'spoofing', 'cracking', 'Phishing' and any other type of malicious or mischievous activity against any network and computing

resource user, any host on the CIA Network, or any other host on the Internet by any member of the CIA community will be grounds for immediate removal of said individual user access and devices from the CIA network and may be subject to further legal action

K. Harmful Activities

All harmful activities are prohibited, including, but not limited to the following: 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;
9. Providing your password to another; and
10. 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 ITS; 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 the 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, network systems, and 3rd party cloud-hosted solutions are CIA-owned resources and business tools used only by authorized persons for CIA business and academic purposes. Therefore, any personal information, files, program, or other personal data stored or installed on a CIA computing or 3rd party cloud-hosted resource is CIA property. Thus, the CIA retains the right to access and review this information as deemed necessary.

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 pursuits (such as faculty publishing activities);
3. Political campaigning;
4. Commercial or personal advertising
5. Personal communications and file storage; and
6. The personal gain or benefit of the user.

SECURITY

A. System Administration Access

Certain system administrators of the CIA's systems will be granted authority to access files to maintain the systems and backup of information. All privileged account users will have specific accounts created for such privileges. The CIA avoids the use of generic user accounts unless a business need is identified and documented.

Based on ongoing risk assessments, periodic internal audits of user privileges and administrative access logs are conducted for designated systems (for example, systems with sensitive personally identifiable or financial information).

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 ITS management, subject to CIA approval.

C. Availability

ITS will make every effort to ensure the operation of the CIA network and the integrity of the data it contains. To perform needed repairs or system upgrades, ITS may, from time to time, limit network access and/or computing resources for regular or unexpected system maintenance. ITS 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. Ensuring users complete any required training;
4. Encouraging users to save all files to a CIA network drive (network drives are backed up every day where local drives are not); and
5. Notification of personnel changes.

E. Wireless Access Points

The Information Technology department provides wireless services for use by CIA faculty, students, and staff. Since wireless is provided centrally by ITS, the installation of private wireless access points (APs) and other devices used to boost wireless signal coverage is not allowed on campus. These devices can and do interfere with the CIA's centrally provided wireless network system. The ITS department will take steps to shut down any personal network access devices used.

F. Virus Protection and Device Security

All CIA computers, including servers, utilize virus detection software. All personal devices such as desktops, laptops, or any other device that may access the CIA network are required to utilize a fully functioning and updated virus detection software application. In addition, all personal devices must be fully updated with the most recent vendor-supplied security patches.

G. Public Information Services

Departments and individuals may, with the permission of the Vice President – Chief of Staff & Information Technology of the CIA, configure computing systems to provide information retrieval services to the public at large under the auspices of the CIA. However, in so doing, particular attention must be paid to issues addressed earlier in this policy, such as authorized use, responsible use of resources, and individual and departmental responsibilities. In addition, copyrighted information and materials and licensed software must be used in an appropriate and lawful manner.

MOBILE COMMUNICATION DEVICES

Users who have a valid business need to use an MCD may be authorized by their department head and/or cabinet member to be issued with such equipment. The department head is responsible for reviewing this authorization annually. All devices authorized for CIA employee use must then be approved by the Vice President – Chief of Staff & Information Technology. All MCD must be purchased and managed by the ITS Department using the CIA's corporate program.

COMPUTER HARDWARE, TELECOM EQUIPMENT AND SOFTWARE ACQUISITIONS

All acquisitions of computer hardware, telecom equipment, software, 3rd party hosted software, and peripheral devices are managed by the ITS Department. The Information Technology Department must initiate all purchasing of said items. Upon delivery, the ITS Department personnel will receive, inventory, configure and deploy all computer hardware, software, networking, and Mobile Communication Devices.

All purchases (new or upgrade) requests must be made in writing to the VP- Chief of Staff and Information Technology by a department head or cabinet member.

PROCEDURES AND SANCTIONS

A. Responding to Security and Abuse Incidents

All users and departmental units are responsible for reporting any discovered unauthorized access attempts or other improper usages 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 notify the same to such user's department head, Human Resources and/or the 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 substantive changes to the policy have been made and the policy and all amendments will be available via the CIA portal.

E. RESPONSIBLE CABINET MEMBER

Vice President – Chief of Staff & Information Technology: 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
HSMD 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, 3/29/2022

_____

Board Approval to Proceed (if required), Date

_____

Cabinet Approval to Proceed: 12/3/2018, 4/7/2022

_____ _____

Policy Revision Dates:

_____

Scheduled Review Date: