Student Computer and Network Usage Policy

Purpose

This is a college-wide policy adopted by The Culinary Institute of America (CIA) to allow for the proper use and management of all CIA computing and network resources. These guidelines pertain to all CIA campuses regardless of the networks or systems operated.

The CIA grants access to its networks and computer systems subject to certain responsibilities and obligations set forth herein and subject to all local, state, and federal laws. Appropriate use should always be legal, ethical, and consistent with the CIA's mission.

Users must realize that providing access is a privilege provided by the CIA and should be treated as such. Enforcement of established rules will help provide a benefit to all users.

Information Technology Services (ITS) views the CIA's network and computing resources as shared resources and their use as a privilege. The primary purpose of these resources is to allow access to information that will support the CIA administration, educational process, and mission. Thus, network abuse or applications that inhibit or interfere with the use of the network by others are not permitted.

Individual Responsibilities

Common Courtesy and Respect for Rights of Others

All users are responsible for respecting and valuing the privacy of others, behaving 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.

Communications on CIA computers (which includes any personal devices registered on the CIA network, regardless of ownership) or networks should always be businesslike, courteous, and civil. Such systems must not be used for the expression of hostility or bias against individuals or groups; offensive material such as obscenity, vulgarity or profanity; inappropriate jokes; or other non-businesslike material. Sexually explicit material, cursing, and name-calling are not appropriate communications. Users who engage in such activity will be subject to disciplinary action.

Content

Users who make use of forums, 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.

Copyright Infringement and Peer-to-Peer File Sharing

Under the Digital Millennium Copyright Act and Higher Education Opportunity Act (H.R. 4137), illegal distribution of copyrighted materials may be punishable by law. These materials include, but are not limited to, the unauthorized distribution of songs, videos, games, textbooks, or other type of creative content.

In addition to any other charges that might be brought against you, the copyright holder can file suit, which can result in legal fees and damages that must be paid.

Therefore, peer-to-peer file sharing is not allowed and is blocked on the CIA network using bandwidth-shaping technology. The CIA is legally obligated to assist authorities in identifying individuals who violate copyright law pertaining to peer-to-peer file sharing. It is also in violation of the college's policy to use technology designed to circumvent the blocking of this activity.

Responsible Use

All users are responsible for refraining from all acts that waste CIA computer or network resources or prevent others from using them. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with or used by others.

Permitting Unauthorized Access

All users are prohibited from running or otherwise configuring software or hardware to intentionally allow access by unauthorized users.

Termination of Access

At the time you cease being a member of the CIA community, you may not use facilities, accounts, access codes, privileges, or information for which you are not authorized.

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 ITS system administration personnel.

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.

Denial of Service Attacks

Denial of service attacks, "fire-bombing," "flaming," "hacking," "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's network, or any other host on the Internet by any member of the CIA community will be grounds for immediate removal of said individual from the CIA network.

Harmful Activities

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

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 frivolous or excessive messages (e.g., chain letters), (5) gaining unauthorized access to CIA computing and networking systems, (6) using a password without authority, (7) utilizing potential loopholes in the CIA's computer security systems without authority, and (8) using another user's password.

Tampering of Equipment or Resources

No computer equipment, including peripherals, 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.

Use of Licensed Software/Downloading

No software may be installed, copied, or used on CIA resources except as permitted by ITS. 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.

Network and computer resource users in the residence halls are responsible for the physical and software security of their personal computers. The registered owner of the computer will be held responsible for any violation of CIA or ITS policies traced back to the computer, regardless of whether or not the owner personally committed the violations.

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 pursuits (such as faculty publishing activities), (3) political campaigning, (4) commercial or personal advertising, or (5) the personal gain or benefit of the user.

Responsibilities

The owner of the computer must be present whenever ITS personnel work on it. Before work will be done on your machine, you will sign a waiver releasing ITS from any liability.

Machines must meet or exceed minimum requirements for both hardware and software before an ITS staff member will do any work on them. See Technology on Campus, Wireless Network for the details of these requirements. Any machine that requires ITS support will be verified as in full working condition before and after ITS does any work.

It is your responsibility to maintain and update virus and spyware software on your computer to avoid any Internet or wireless network performance issues.

Security

System Administration Access

Certain system administrators of the CIA's systems will be granted authority to access files for the maintenance of the systems, as well as storage or backup of information.

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.

Availability

ITS will make every effort to ensure the operation of the CIA network and the integrity of the data it contains. In order 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.

As a CIA student, you waive the right to compensation for lost work or time that may arise from these shutdowns. Neither the CIA nor ITS can compensate you for degradation or loss of personal data, software, or hardware as a result of your use of CIA-owned systems or networks, or as a result of assistance you may seek from ITS personnel. You are responsible for making backup copies of your computer files.

Wireless Access Points

The Information Technology Department provides wireless service for use by students. Wireless access is also available to faculty, staff, and guests. 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 we detect.

Virus Protection and Device Security

All CIA computers, including file servers, utilize virus detection software. All personal devices such as desktops, laptops, or any other devices that may compromise the security of 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.

Amendments

The Culinary Institute of America and Information Technology Services reserve the right to amend the policies herein as needed. Users will receive copies of these amendments whenever possible.

Should it be determined that network traffic being generated from any connection is drastically inhibiting or interfering with the use of the CIA's network and computing resources by others, the college reserves the right to terminate any user's access without notice.

Authorized Use

An authorized user is any student who has been granted access by the CIA to its computing and network resources and whose usage complies with this policy.

Privacy

Users must recognize that there is no guarantee of privacy associated with their use of CIA network and computer systems. The CIA may find it necessary to view electronic data and it may be required by law to allow third parties to do so (e.g., electronically stored data may become evidence in legal proceedings). It is also possible that messages or data may be inadvertently viewed by others.

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.