


ACCEPTABLE USE POLICY (AUP)

Revision History

Document No:	Version:	Revised by:	Section Revised
ITPO-019	1.0	Information Security Team	Sections 1, 2, 3, 4, and 5

Document Control

Approved by Name:	Approved by Name / Signature:	Approved Date:	Next Review Date:
Sr. CIEE Policy Review Committee	William Magaw 	16 Aug 2018	16 Aug 2019



Contents

1	Overview	3
2	Purpose	3
3	Scope.....	3
4	Policy.....	4
4.1	General Use and Ownership	4
4.2	System and Network Use	5
4.3	E-mail and Internet Use	7
4.4	Social Media Use	9
5	Policy Compliance	10
5.1	Compliance Measurement.....	10
5.2	Exceptions	10
5.3	Non-Compliance.....	10



1 Overview

CIEE recognizes the importance of an Acceptable Use Policy. This policy is not intended to impose restrictions that are contrary to CIEE's established culture of openness, trust and integrity. It is instead to protect our employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

- **You are expected to read, understand, and follow this Policy.** No single policy can cover all the possible issues you may face. You should seek guidance from your manager or other designated CIEE resource before taking any actions that could create risks or otherwise deviate from this Policy's requirements. CIEE may treat any failure to seek and follow such guidance as a violation of this Policy.

2 Purpose

The purpose of this policy is to outline the Acceptable Use of information, electronic and computing devices, and network resources at CIEE. These rules are in place to protect the employee and CIEE. Inappropriate use exposes CIEE to risks including virus attacks, compromise of network systems, services, and legal issues.

3 Scope

This policy applies to all staff within CIEE (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers and interns engaged with CIEE).

Adherence to this policy is mandatory and non-compliance could lead to disciplinary action, up to and including termination of employment.



4 Policy

When using CIEE's Systems and Network resources to access and use Systems, E-mail, the Internet or Social Media, it is important to realize that you represent the company. All such use and communications, therefore, should be for business-related reasons, demonstrate appropriate and professional judgment, not reflect poorly on CIEE or any of its employees, comply with applicable laws and CIEE's employee conduct policies (including but not limited to the Equal Employment Opportunity and anti-harassment policies), and should not be for personal business.

The following activities are, in general, prohibited. Staff may be exempted from these restrictions during the course of 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 CIEE authorized to engage in any activity that is ***illegal under local, state, federal or international law*** while utilizing CIEE-owned resources.

4.1 General Use and Ownership

- CIEE proprietary information stored in hardcopy, electronic and computing devices whether owned or leased by CIEE, the employee or a third party, remains the sole property of CIEE.
- CIEE reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and may monitor equipment, systems and network traffic at any time.
- You may access, use or share CIEE proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- You have a responsibility to promptly report any theft, loss or unauthorized disclosure of CIEE proprietary information.
- Appropriate use should always be legal and ethical and show respect in the consumption of shared resources.
- Appropriate use should demonstrate respect for system security mechanisms, CIEE's intellectual property and the individuals' rights to privacy in compliance with applicable data privacy laws and data security.
- Each individual is responsible to protect the security and integrity of CIEE information stored on any individual's computing devices.
- All Confidential Data must be encrypted and secure while at rest and while being transmitted.
- All computing devices must be secured with a password-protected screensaver and you must lock the screen or log off when the device is unattended.
- You will not violate any applicable local, state, national or international law or regulation.



4.2 System and Network Use

All CIEE equal employment opportunity and anti-harassment policies apply to System and Network use, and specifically prohibit discriminatory, harassing, offensive, or otherwise improper behavior while using System and Network resources.

CIEE reserves the right to monitor all Systems and Networks without notice.

It is prohibited for any CIEE Staff to:

- Violate 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 CIEE.
- Copy unauthorized copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CIEE or the end user does not have an active license.
- Access Databases, Systems, Networks, Data, Servers or Accounts for any purpose other than conducting CIEE business.
- Export software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Introduce any malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Reveal your CIEE account password to others or allow use of your account by others. This includes family and other household members when work is being done at home.
- Use a CIEE computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Make fraudulent offers of products, items, or services originating from any CIEE account.
- Effect 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, system or account that the employee is not expressly authorized to access.
 - "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Execute any Port scanning or security scanning.
- Execute any form of network monitoring which will intercept data not intended for the employee's host.
- Circumvent user authentication or security of any host, network or account.



- Introduce honeypots, honeynets, or similar technology on the CIEE network.
- Interfere with or deny services to any user other than the employee's host (for example, denial of service attack).
- Use 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.



4.3 E-mail and Internet Use

All CIEE equal employment opportunity and anti-harassment policies apply to the E-mail and Internet system, and specifically prohibit the use of E-mail to send discriminatory, harassing, offensive, or otherwise improper messages.

E-mail should be written in the same manner and with the same care and sensitivity as any other business correspondence.

Any E-mail sent and received at CIEE (or via CIEE's E-mail facilities) is CIEE's property; therefore, all messages are part of CIEE's records. CIEE reserves the right to monitor all messages on the E-mail system without notice.

Unusual E-mail should not be opened; it is especially important not to open an attachment from an unknown source. If opened in error, employees should contact the IT Help desk immediately for assistance.

It is prohibited for any CIEE Staff to:

- Use E-mail or the Internet for personal gain or to solicit non-CIEE business.
- Use E-mail and the Internet to disrupt the operation of CIEE's network.
- Allow E-mail and the Internet to interfere with your daily productivity.
- Send unsolicited E-mail messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (E-mail spam).
- Create or forward "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- E-mail or otherwise transmit any content that is unlawful, harmful, threatening, abusive, harassing, torturous, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically, or otherwise objectionable, containing explicit or graphic descriptions or accounts of sexual acts (including, but not limited to, sexual language of a violent or a threatening nature directed at another individual or group of individuals).
- Use E-mail or the Internet to impersonate any person or entity, including, but not limited to, a CIEE employee or officer, E-mail or falsely state or otherwise misrepresent an affiliation with a person or entity.
- Forge headers or otherwise manipulate identifiers in order to disguise the origin of any content transmitted through CIEE's internet service.
- E-mail or otherwise transmit any content that an employee does not have a right to transmit under any law or under contractual or fiduciary relationships (such as inside information, trade secrets, proprietary and/or confidential information learned or disclosed as part of employment relationships or under non-disclosure agreements).
- E-mail or otherwise transmit any content that infringes any patent, trademark, trade secret,



copyright, right of publicity or other proprietary right of any party.

- E-mail or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.



4.4 Social Media Use

CIEE recognizes that social media can be a valuable way to market its business. Social media consists of websites like Facebook, Twitter, Instagram, LinkedIn, MySpace, blogs, or any other site where one posts or communicates information in a public or quasi-public Internet forum.

- Certain employees may be asked to create or maintain CIEE's social media profiles. An employee may act on behalf of CIEE in the social media context only with express authorization from their supervisor. CIEE has ultimate discretion over the content posted on its social media accounts and may remove or alter content at any time. This policy also applies to the Company website.
- CIEE understands that employees are free to create and maintain personal social media profiles during non-work hours and on non-work equipment.
- Employees generally may not use social media websites on company information systems or during work time unless authorized to do so by a supervisor.
- When and if an employee makes any business-related comment on his/her personal social media, it should be made clear that the comment is made in his or her personal capacity and not as a representative of CIEE.
- Employees may not post material that disparages the services or products provided to the public by the CIEE, and may not comment on CIEE's clients/customers without authorization.
- Employees must comply with all applicable employment policies including CIEE's harassment, discrimination, and confidentiality policies when using social media.
- Employees should refrain from making defamatory, demeaning, discriminatory, harassing, threatening, violent, abusive or obscene related in any way to their employment.
- Any content sent and received using CIEE systems, Network or resources are CIEE's property; therefore, are part of CIEE's records. CIEE reserves the right to monitor all Social Media without notice.
- Unusual contents should not be opened; it is especially important not to open an attachment from an unknown source. If opened in error, employees should contact the IT Help desk immediately for assistance.
- This policy in no way restricts employees' rights to engage in protected concerted activity, such as discussing wages, hours, or other working conditions, through social media.



5 Policy Compliance

5.1 Compliance Measurement

CIEE's Information Security 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.

All activity in CIEE's network is subject to monitoring without notice for abuse, violations of law or employee conduct policies, and illicit activity.

5.2 Exceptions

There are no exceptions to this policy.

5.3 Non-Compliance

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



This page intently left blank



ACKNOWLEDGMENT

[Please sign and return to HR]

Acknowledgment of Receipt and Review

I acknowledge that I received and read a copy of CIEE's **Acceptable Use Policy**, approved on DD-MMM-CCYY and will adhere to the contents of this policy. Furthermore, I understand that any violations of this policy could result in disciplinary actions, up to and including termination of employment or legal action.

This Policy is not a promissory and does not set terms or conditions of employment or create an employment contract.

Signature

Printed Name

____/____/____

Date