User Policy

Introduction

Your Responsibilities as a Computer User

Applicable Policies and Laws

As a condition of employment or collaboration with the Computation Institute (CI), you may have access to various CI computer systems, networks, applications, data or other Information Technology (IT) assets. Before this access is granted, you must agree to abide by usage and access policies and to use CI IT resources in a responsible and ethical manner, as described below. Please read this information carefully. You are required to acknowledge your acceptance of this agreement to abide by the conditions set forth below.

Violators of these standards may be subject to disciplinary action up to and including dismissal and/or account termination

Your Responsibilities as a Computer User

The following principals govern the use of CI IT assets. Users are expected to abide by these principles.

- You are responsible for the proper use of the tools each computer system provides and for confidentiality of information entrusted to you.
- Your computer accounts are assigned to you alone and should not be shared with anyone, including coworkers, trainers, or computer support staff. You must protect your passwords, choose complex passwords and change them regularly in accordance with CI policies.
- You must not use CI IT resources for illegal or malicious purposes, such as harassment of others, disruption or unauthorized monitoring of electronic communications or unauthorized copying of copyrighted materials.
- You must refrain from unethical usage, including: unauthorized use of computer accounts and resources assigned to others, use of computing facilities for private business or political purposes or private gain, academic or scientific dishonesty, or violation of software licenses.
- You will respect the confidentiality and privacy of individuals to whose records you may have access in accordance with CI policy, ethical standards, and state and federal laws.
- You will be expected to read, understand, and comply with (as appropriate) any requests relating to cyber or information security.
- You should report any breach of security, policy violation, or suspicious activity to security@ci.uchicago.edu and/or your supervisor or sponsor.
- You should be aware that any or all computer and network systems and files on these systems may be monitored by appropriate authorities.

Applicable Policies and Laws

- Eligibility and Acceptable Use Policy for Information Technology
  - The University of Chicago policy defining roles, responsibilities, and restrictions of University resources and technologies.
- Digital Millenium Copyright Act of 1998
  - A United States copyright law which criminalizes production and dissemination of technology that can circumvent measures taken to protect copyright, not merely infringement of copyright itself, and heightens the penalties for copyright infringement on the Internet.
- Computer Fraud and Abuse Act of 1986
  - A United States law which criminalizes knowingly or intentionally accessing a computer without authorization to obtain sensitive data, with the intent to defraud, or with the intent to disrupt or destroy services or data.
- National Information Infrastructure Protection Act of 1996
  - Strengthens the Computer Fraud and Abuse Act by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks.