CIF Acceptable Use Policy

Bryan Jacobs

January 25, 2008

Abstract

This purpose of this document is to clearly elaborate what constitutes acceptable use of the Computer Interest Floor's technological systems and resources.

0.1 Rochester AUP

You are not required to abide by the University of Rochester Network Acceptable Use Policy document when using CIF systems and resources.

However, when you make use of the University of Rochester's network or resources indirectly via CIF systems, such as when accessing the campus network or internet via a CIF router, the terms and conditions of that document apply IN ADDITION TO the ones stated herein. Where conflicts exist, that document shall take precedence over this one. You are required to have obtained, read, understood, and consented to the most recent copy of that document prior to using any University of Rochester resources, directly or indirectly.

0.2 Identity Information

You are responsible for protecting your passwords, certificates, numeric identifiers, and other personal information. The CIF Tech Staff will do their best to ensure that such information is not compromised when within the appropriate locations of CIF systems or when in transit between those appropriate locations. If you at any time feel that your identity information is being stored in an insecure manner, or that your identity information has been or will be compromised, contact the Tech Director with your complaints. Provided that you have not lodged a complaint, you are responsible for ALL activity conducted by an individual who provides your identity information. This INCLUDES cases where your identity information was obtained by guessing or brute force.

You may not attempt to compromise another's identity information.

0.3 Appropriate Access

If access to a resource was not intentionally granted you by the Tech Director, or you have reason to believe such access was granted, you are not permitted to access that resource. You shall not attempt to do so.

0.4 Discovery of Vulnerabilities

If you discover a vulnerability or unintended behavior in a CIF resource, you shall immediately notify the Tech Director, without exception. You shall not attempt to exploit or "test" the vulnerability.

0.5 Profanity and Obscenity

You may not use CIF resources to transmit or store obscene or profane materials where so doing causes discomfort or unease in another.

0.6   Legality

You may not use CIF resources in a way inconsistent with all applicable laws, excluding none.

You may also not use CIF resources in a way inconsistent with the University of Rochester's rules for student conduct. This does not include their Acceptable Network Use Policy except where noted above.

0.7   Malicious Use and Denial of Service

Because CIF's technological resources are shared, you may not use any system with the intent to deny another their legitimate use of that (or any other CIF) system, except where you have the prior explicit consent of the Tech Director.

You may also not use the systems in a way that causes a Denial of Service, such as consuming an unreasonably large share of system resources.

0.8   Entitlement

- You are entitled to have useful, educational, and enjoyable technological resources provided you by the CIF Tech Staff as they see fit.

- You are NOT entitled to have access to all CIF systems and resources.

- Provided that you have not violated the terms of this document or otherwise engaged in conduct detractive to CIF, your access shall not be curtailed beyond that of any other individual with your affiliation with CIF.

- In the event that you do violate the terms of this document or another which you have read and acknowledged, your ability to access resources may be restricted or removed by the Tech Director.

0.9   Definitions

- In all cases in this document, "Tech Director" means the CIF elected Tech Director or his/her designated proxy.

- "resource" means "service, system, device, network, item, or information"