ACCEPTABLE USE POLICY
NETWORK SERVICES

INTRODUCTION

Cybera is committed to being a conscientious network operator. To support us in preserving the value and enjoyment of the network, Members agree to be bound by the terms of this Network Services Acceptable Use Policy ("AUP").

Except where otherwise indicated, the "Member" refers to the organization that accesses Cybera services. By using services provided by Cybera ("Services"), Members agree to comply with the AUP for Network Services outlined in this agreement.

If the Member does not agree to be bound by the AUP, the Member should immediately stop using the Services and notify Cybera of termination.

If you have questions about this AUP, please e-mail: policy@cybera.ca.

GENERAL

Cybera recognizes that no one owns or controls the internet. Cybera can neither monitor nor control activities of Cybera Members and their end-users. Cybera does not actively screen, review, censor, edit or take responsibility for the activities or content of Cybera Members. Members, not Cybera, assume all responsibility relating to their internet activities.

Cybera may amend this AUP at any time by posting notice of the amendment on the Cybera website or by sending notice via email to the primary email address associated with the Member. Any such modification shall be effective as of the earlier of the date of posting of the modified AUP or the date identified in the email. Continued use of Cybera services following any announced changes shall constitute acceptance of those changes by the Member.

This AUP supplements the Cybera Membership Agreement. Any violation of this AUP will constitute a violation of Cybera membership, internet buying group, and peering agreements.

Members should be aware that Cybera is a not-for-profit company. As such, Cybera offers services on a best efforts basis unless otherwise defined by a separate contract with Cybera. Members must exercise a high degree of judgment and responsibility with respect to their use of the Services, including the responsibility to comply with this AUP.

PROHIBITED ACTIVITIES & ABUSE

Using the Cybera network in a way that has a material adverse effect on other Cybera Members is strictly prohibited. Cybera reserves the right to terminate or disconnect services if the Member engages in prohibited activities. Without limitation, the Member may not use (or allow anyone else to use) Cybera's services to:

I. Transmit, disseminate, or otherwise infringe on copyright, patents, trademarks, trade secrets, or other intellectual property including but not limited to: illegally acquired pirated computer programs, cracker utilities, warez and software serial numbers or registration codes
II. Violate any law, statute, ordinance or regulation governing the client's or Cybera's business or

activities

III. Promote or teach illegal activities
IV. Attempt to use the Services in such a manner so as to avoid incurring charges
V. Gain or attempt to gain unauthorized access to servers or services. Such attempts include but are not limited to:
    A. Phishing scams
    B. Password robbery
    C. Security hole scanning
    D. Port scanning
    E. Probing, monitoring or testing for system or network vulnerabilities
    F. Introducing viruses, trojan horses, trap doors, back doors, easter eggs, worms, time bombs, packet bombs, cancel bots or other computer programs that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or personal information.
    G. Intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return addressing information, and IP addresses
    H. Running bots or clients for malicious or illegal purposes
    I. Undertaking denial of service attacks

SPAM OR UNSOLICITED COMMERCIAL EMAIL

Cybera has a zero tolerance policy for the sending of spam or unsolicited commercial email (UCE) over the Cybera network. Members will use reasonable efforts not to send spam or UCE (and to educate its end users accordingly). Members are also responsible for ensuring that their end-users adhere to this AUP, and must take reasonable precautions to secure their servers and sites against spam exploits.

VIOLATION OF THIS ACCEPTABLE USE POLICY

Upon detection or notification of a violation of this AUP, Cybera may without notice temporarily restrict access to the Cybera network (when the incident cannot be isolated to an offending Member incident) or shut down the offending systems. Cybera may cancel a Member's network services if the Member is found in violation of this AUP.

ADMINISTRATIVE ACCOUNTS AND MANAGEMENT SOFTWARE

To facilitate data center, network, and server management and related activities, Cybera maintains administrative accounts and passwords. Reasonable precautions are made by Cybera to maintain the security of these accounts, the related tools and the privacy of client data. Clients should not tamper, hinder, delete, or in anyway change the functioning of these tools or accounts. To do so intentionally or otherwise is a violation of this agreement and is grounds for the immediate termination of Services.

Cybera staff will not use their permissions or privileges to invade the privacy of Members or their end-users. It is possible that in the normal course of their duties information of a personal or confidential nature may be accessed or viewed. Cybera staff will handle the information in a professional manner and maintain confidentiality. Please refer to the Cybera Privacy Notice for more information.

COMPLAINTS

Please direct comments, questions, and complaints of violations related to this AUP to policy@cybera.ca.