

# ACCEPTABLE USE POLICY

## CLOUD SERVICES

### INTRODUCTION

Cybera is committed to being a conscientious cloud operator. To support us in preserving the value and enjoyment of Cybera's cloud services, users agree to be bound by the terms of this Acceptable Use Policy ("AUP").

Except where otherwise indicated, "User" refers to each person who accesses Cybera's cloud services. By using cloud services ("Services") provided by Cybera, Users agree to comply with the AUP for cloud services outlined in this agreement.

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

If you have any questions about this AUP, please e-mail: [policy@cybera.ca](mailto:policy@cybera.ca).

### GENERAL

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

Cybera may amend this AUP at any time by posting notice of the amendment on Cybera's website or by sending notice via email to the primary email address associated with the Services. 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's Services following any announced changes shall constitute acceptance of those changes by the User.

This AUP supplements the Cybera [Rapid Access Cloud Terms of Service](#). Any violation of this AUP will constitute a violation of the terms of service.

### PROHIBITED ACTIVITIES & ABUSE

Using the Cybera network or Cybera hosted systems or virtual services in any way that adversely affects other Cybera members or Users is strictly prohibited. Cybera reserves the right to terminate or disconnect services if the User engages in prohibited activities. Without limitation, the User 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: pirated computer programs, cracker utilities, warez and software serial numbers or registration codes;
- II. violate any law, statute, ordinance or regulation governing the User'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. copy, distribute, sub-license or otherwise make available any software or content Cybera provides or makes available to the User, or which the User obtains through the Services, except as authorized by Cybera;
- VI. 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.

## UNLAWFUL OR INAPPROPRIATE CONTENT

Cybera reserves the right to move or remove content or links to content, in whole or in part, that it deems unacceptable or in violation of the terms of this AUP. This includes content or links to content which:

- I. is unlawful;
- II. defamatory, fraudulent, or deceptive;
- III. obscene, profane, or pornographic;
- IV. promotes injury or physical harm against any group or individual;
- V. promotes or teaches illegal activities.
- VI. violates any law, statute, ordinance or regulation governing the User's business or activities.

## 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. Users will use commercially reasonable efforts not to send spam or UCE (and to educate its end users accordingly). The User agrees not to host sites or information used by spammers. Users are also responsible for ensuring that their end-users adhere to this AUP, and shall take reasonable precautions to secure their servers and sites against spam exploits.

## 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 User data. Users cannot 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 Users or their 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



complete confidentiality. Please refer to Cybera's [Privacy Notice](#) for more information.

## **VIOLATION OF THIS ACCEPTABLE USE POLICY**

The User acknowledges that misuse of Cybera's Services or violation of the AUP can lead to temporary or permanent disabling of accounts and administrative or legal actions. Upon detection or notification of a violation of this AUP Cybera may without notice temporarily restrict access to Cybera's network (when the incident cannot be isolated to an offending User incident) or shutdown offending systems. Cybera may initiate an investigation and take action.

## **SERVICE TERMINATION**

This AUP is not exhaustive. Cybera reserves the right to refuse service to anyone at any time without warning or prior notice.

## **COMPLAINTS**

Please direct comments, questions, and complaints of violations related to this AUP to [policy@cybera.ca](mailto:policy@cybera.ca).