Acceptable User Policy

Industry Sandbox & Artificial Intelligence Computing (ISAIC) is committed to being a conscientious cloud operator. To support us in preserving the value and ease of use of the ISAIC'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 the ISAIC's cloud services. By using cloud services ("Services") provided by the ISAIC, Users agree to comply with the AUP for cloud services outlined in this agreement. Note that the terms tenant, user and client are used interchangeably to refer to the party accessing the ISAIC services or programs.

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

If you have any questions or require further clarification about this AUP, please e-mail: isaic@ualberta.ca.

GENERAL

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

The ISAIC may amend this AUP at any time by posting notice of the amendment on the ISAIC'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 the ISAIC's Services following any announced changes shall constitute acceptance of those changes by the User.

This AUP supplements the ISAIC's Terms of Services. Any violation of this AUP will constitute a violation of the terms of service.

ACCEPTABLE ACTIVITIES & USE

This section describes uses of the ISAIC information technology systems that are considered acceptable by the ISAIC management. The general criteria used in deciding acceptable use are whether it serves the ISAIC's stated purpose and goals, whether it complies with government laws and regulations, and whether it does not adversely affect others. The ISAIC allows the use of its services and resources as long as that use does not interfere with official business, unexpectedly and/or unreasonably increases cost to the ISAIC or exposes the ISAIC to undue risk, including reputational. Questions about the use of the ISAIC resources that are not explicitly mentioned in this policy should be directed to the ISAIC management.

The ISAIC resources may be used in the conduct of operations and/or research. Examples of such use of the ISAIC resources include, but are not limited to:

- Computation and modeling, and support of experiments needed to accomplish User research, including research on information technology systems;
- Analysis and short-term storage of data, including experimental data, output from models, and administrative data (please see the Terms of Services document for data storage and retention information);
- Preparation of data and information generated on ISAIC resources to be shared (e.g. in reports, papers, memos, correspondence, databases, graphics, displays, presentations etc.);

The ISAIC resources may be used to communicate and exchange information with others located outside of the ISAIC to share data or information related to the identified and agreed to project submitted by the User to the ISAIC. This includes researchers at other institutions, customers in industry and elsewhere, vendors and companies with products of interest to the User, other government agencies, and the public.

Software from the Internet and other public sources, and installing unnecessary software from any source, increases security risks to the ISAIC networks and computers by potentially including things such as harmful viruses, back doors, and mechanisms specifically designed to defeat firewall protection. ISAIC staff will be responsible for the initial set-up of a virtual machine and can, if requested, make a copy/clone of a set-up prior to granting access to the User. This would allow for a reset of a system (but would not include a copy of any data generated after the handover) in the event a User identifies a breach or system instability issue.

The ISAIC encourages users to:

- Only install software that will be used for work-related functions.
- Only install or run software that was written by well-known, established sources. At a minimum, you should be able to identify the original source of the software and validate that you can locate and communicate with the author or company to discuss problems that might arise.
- Scan downloaded files for viruses before installing and running them. Generally `shrink-wrapped' commercial software should be free from viruses (although some manufacturers have distributed infected software).

PROHIBITED ACTIVITIES & ABUSE

Using the ISAIC network, Hub hosted systems or virtual services in any way that adversely affects other ISAIC members or Users is strictly prohibited. The ISAIC 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) the ISAIC's services to:

1. 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;

2. violate any law, statute, ordinance or regulation governing the User’s or the ISAIC’s business or activities;

3. promote or teach illegal activities;

4. attempt to use the services in such a manner so as to avoid incurring charges;

5. copy, distribute, sub-license or otherwise make available any software or content that the ISAIC provides or makes available to the User, or which the User obtains through the Services, except as authorized by the ISAIC;

6. take advantage of technicalities, loopholes, and ambiguous language in this or other ISAIC agreements (e.g. Terms of Service);

7. reveal your account password to others or allowing use of your account by others.This includes family and other household members when work is being done at home;

8. use the ISAIC 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;

9. effect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. execute any form of network monitoring which will intercept data not intended for the User’s host, unless this activity is a part of a normal job/duty.

11. provide public access to application user interfaces (UI) without some form of access control or authentication.

12. gain or attempt to gain unauthorized access to servers or services. Such attempts include but are not limited to:

    1. Phishing scams

    2. Password robbery

    3. Security hole scanning

    4. Port scanning

    5. Probing, monitoring or testing for system or network vulnerabilities.

6. 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.

7. Intentionally omitting, deleting, forging or misrepresenting transmission information, including headers, return addressing information and IP addresses.

8. Running bots or clients for malicious or illegal purposes

9. Undertaking denial of service attacks.

UNLAWFUL OR INAPPROPRIATE CONTENT

The ISAIC 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:

1. is unlawful;

2. defamatory, fraudulent, or deceptive;

3. obscene, profane, or pornographic;

4. promotes injury or physical harm against any group or individual;

5. promotes or teaches illegal activities.

6. violates any law, statute, ordinance or regulation governing the User's business or activities.

SPAM OR UNSOLICITED COMMERCIAL EMAIL

The ISAIC has a zero tolerance policy for the sending of spam or Unsolicited Commercial Email ("UCE") with the aid of ISAIC resources or as a result of work involving the ISAIC. The ISAIC retains the right to terminate services if Users are determined to violate this policy.

ADMINISTRATIVE ACCOUNTS AND MANAGEMENT SOFTWARE

The ISAIC does not maintain administrative accounts and passwords to User accounts. It is therefore the responsibility of the User to make reasonable precautions to maintain the security of their account, the related tools and the privacy of User-generated data.

Users are not to tamper, hinder, delete, or in any way change the functioning of the provided tools or software accounts that enable use of AI software provided by the ISAIC. To do so

intentionally or otherwise is a violation of this agreement and is grounds for the immediate termination of Services.

The ISAIC 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. The ISAIC staff will handle the information in a professional manner and maintain complete confidentiality.

VIOLATION OF THIS ACCEPTABLE USE POLICY

The User acknowledges that misuse of the ISAIC'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, the ISAIC may without notice temporarily restrict access to the ISAIC's resources (when the incident cannot be isolated to an offending User incident) or shutdown offending systems. The ISAIC may initiate an investigation and take action.

SERVICE TERMINATION

This AUP is not exhaustive. The ISAIC reserves the right to refuse service to anyone at any time without warning or prior notice. Please see the ISAIC's - Terms of Service - section 11: Termination for more details.

COMPLAINTS OR QUESTIONS

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