ILAC INTERNATIONAL HIGH SCHOOL

Pathway to Higher Education

IT Security Policy

This IT Security Policy is a valuable guideline by which faculty, staff, and Students can review the requirements of legal and ethical behavior within the IIHS community when using a computer, computer system, or the network. Headings and numbering are for ease or reference only.

Purpose

1. As a part of its commitment to achieving desired learning outcomes, IIHS acquires and maintains computers, computer systems, programs, and networks. It also outsources secure synchronous and asynchronous programs and program modules which form part of the IIHS curriculum. These computing resources are intended for IIHS -related purposes, including direct and indirect support of IIHS 's learning outcomes; of IIHS administrative functions; of Student and campus life activities; and of the free exchange of ideas among members of the IIHS community and between the IIHS community and external communities.

2. The use of IIHS computing resources (which includes outsourced programs and program modules), like the use of any other IIHS -provided resource and like any other IIHS -related activity, is subject to the normal requirements of legal and ethical behavior within the IIHS community. Thus, permitted use of a computer, computer system, or network does not extend to whatever is technically possible. For Students, a breach of this policy may lead to a range of discipline, including expulsion in the most severe of circumstances. For faculty and staff, breaches of the policy can also lead to a range of discipline, including dismissal in the most severe cases.

3. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Who is Bound

4. This policy applies to all users of IIHS computing resources (including but not limited to Students, faculty, and staff, or whether affiliated with the IIHS or not, and to all uses of those resources, whether on campus or from remote locations.

5. The IIHS may also take action relating to a Student's or staff member’s use of IIHS or non- IIHS computer resources, either on campus or elsewhere, when such behavior may involve the commission of a crime or poses a danger to others or is in contravention of any IIHS policy.

Policies on the Use of IIHS Computing Resources

6. Users must comply with all municipal, provincial, federal and other applicable laws; as well as all generally applicable IIHS rules and policies. Examples of such potentially applicable laws, rules and policies include the laws of libel, privacy, copyright, trademark, obscenity and child pornography; the Ontario Freedom of Information and Protection of

Personal Privacy Act; the Personal Information Protection and Electronic Documents Act and the Criminal Code of Canada, which, while it does not specifically name them, prohibits the intent of "hacking", "cracking", and similar activities; and each of IIHS's policies to which Students, faculty and staff are specifically bound.

7. Users who engage in electronic communications with persons in other provinces or countries or on other systems or networks should be aware that they may also be subject to the laws of those other provinces and countries and the rules and policies of those other systems and networks. Users must be sure that the use of any downloaded material (including print, audio, and video) stored on IIHS or a personal computer is not in violation of copyright laws.

8. Users are responsible for complying with the requirements of the contracts and licenses applicable to the software files and other data they install on IIHS or personal systems. Proof of legal licensing should be available upon request. Users may utilize only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.

9. Accounts and passwords should not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the IIHS -- not even with family members or a partner.

10. Users must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so.

11. Users must respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all users of IIHS computing resources, the IIHS may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all the relevant circumstances.

12. IIHS computing and network resources and services may be used only by authorized persons for IIHS-related purposes, including those listed in the Purpose section above. These resources may not be used for other purposes except as authorized by IIHS. For example, the reselling of network services or other uses of computer resources for personal financial gain is not permitted.

13. Use of computers and networks for personal purposes such as email and web access is allowed as a privilege, as long as it does not interfere with work responsibilities, does not place a burden on resources, is done on the individual's own time and conforms to IIHS policies. Personal use is a privilege, not a right, and therefore users are expected to respect the priority of IIHS business and keep personal use to a minimum.

14. Mass emailing or spamming of sub-populations in the IIHS community are not allowed.

15. Individuals may not state or imply that they speak on behalf of IIHS and may not use IIHS trademarks and logos without authorization to do so. Affiliation with IIHS does not, by itself, imply authorization to speak on behalf of IIHS. Authorization to use IIHS trademarks and logos on IIHS computing resources must be obtained prior to their use. The use of appropriate disclaimers is encouraged e.g. "the thoughts expressed here are my personal opinion and do not represent the position of IIHS in any way."

16. The IIHS may temporarily suspend or block access to an account, prior to the initiation or completion of an investigation, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of IIHS or other computing resources or to protect the IIHS from liability.

17. The IIHS may also refer suspected violations of applicable law to appropriate law enforcement agencies. Users who violate this policy may be subject to disciplinary action, and may be denied further access to IIHS computing resources. Disciplinary action may vary depending on the violation and pursuant to IIHS's other policies.

18. The IIHS employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the IIHS cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly. Users should also be aware that their uses of IIHS computing resources are not guaranteed to be private. While the IIHS does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the IIHS's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. The IIHS may also specifically monitor the activity and accounts of individual users of IIHS computing resources, including individual login sessions and communications, without notice, when:

    a. The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;

    b. It reasonably appears necessary to do so to protect the integrity, security, or functionality of IIHS or other computing resources or to protect IIHS from liability;

    c. There is reasonable cause to believe that the user has violated, or is violating, this policy;

    d. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns;

    e. It is otherwise required or permitted by law.

19. IIHS, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate IIHS personnel and/or municipal, provincial or federal law enforcement agencies and may use those results in appropriate IIHS disciplinary proceedings or in litigation.

20. IIHS has the right to change this policy as necessary with reasonable notice to those impacted, including Students.

21. "Cyberspace" is not a separate legal jurisdiction, and it is not exempt from the normal requirements of legal and ethical behavior within the IIHS community. A good rule of thumb to keep in mind is that conduct that would be illegal or a violation of IIHS policy in the "off-line" world will still be illegal or a violation of IIHS policy when it occurs online. The online world is not limited to IIHS.

22. Computer users who engage in electronic communications with persons in other provinces or countries or on other systems or networks may also be subject to the laws of those other provinces and countries and the rules and policies of those other systems and networks. It is therefore impossible to list and describe every law and policy that applies to the use of IIHS computing resources and the Internet - since, by and large, they all do - but the following are some of the ones that most frequently cause problems: Copyright Law Copyright law generally gives authors, artists, composers, and other such creators the exclusive right to copy, distribute, modify, and display their works or to authorize other people to do so. Moreover, their works are protected by copyright from the moment that they are created, regardless of whether they are registered with the Canadian Intellectual Property Office and regardless of whether they are marked with a copyright notice or symbol ©. That means that virtually every email message, web page, or other computer work you have ever created - or seen - is copyrighted. That also means that, if you are not the copyright owner (and bearing in mind this is in no way legal or any kind of advice to you from IIHS), you may not copy, distribute, modify, or display it unless one or more of the following is true:

    a. Its copyright owner has given you permission to do so;

    b. It is in the public domain;

    c. Doing so would constitute fair use;

    d. You have an implied license to do so.

If none of these exceptions apply, your use of the material constitutes copyright infringement, and you could be liable under federal law for fines and damages for each use.

23. For further information about your use of IIHS computing resources and the corresponding protection of your data, it's best to ask before proceeding. You can contact Amy McGrath at amymcgrath@IIHSprogram.ca.

24. Email services are provided to the IIHS community in support of the teaching, learning and research mission of the IIHS and the administrative functions to carry out that mission.

25. This policy and related policies provide the framework in which all email services are provided and used at IIHS.

Definitions Relating to Accounts and Passwords

(a) **Email account:** An email account is the location where mail is actually delivered. It is a combination of a login username and password and disk space. A person may have several email accounts on different computers or email servers. Users are to take precautions to prevent the unauthorized use of email account passwords. Passwords are not to be shared with others and their confidentiality is to be strictly maintained.

(b) **Email username:** The actual name of the account as typed in at the Username prompt when logging onto email.

(c) **Email name address:** The email address is the name address or alias (example: janedoe@protonmail.com) It is linked to a preferred email account but is, itself, not an account username, but rather a permanent email alias.

Choice of Passwords

26. In choosing passwords, users should select codes that are difficult to guess and should change them on a regular basis. Users will be held accountable for all actions performed with their passwords, including those performed by other individuals as a result of user negligence in protecting codes.

27. No one is to use another individual's account, with or without permission. Email accounts can be immediately locked at the request of IIHS, or alternatively blocked by IIHS.

28. Commercial use of mailing lists, except for authorized IIHS business is prohibited.

29. Users are not advised to send confidential IIHS communications (as determined by law, policy, etc.) via email. While IIHS will make every attempt to keep your data private and secure, here are a few examples of when email confidentiality cannot be guaranteed:

    a. Email may be subject to disclosure in accordance with the law.

    b. Back-up copies may be retained for periods of time and in locations unknown to senders and recipients even if the user has deleted it from their account or PC.

    c. In the course of routine systems maintenance, troubleshooting and mail delivery problem resolution, network or systems staff may inadvertently see the content of email messages.

It is the user's responsibility to back up copies of their own email.