

# Anti-Virus Policy

## Purpose

To establish requirements which must be met by all computers connected to lab networks to ensure effective virus detection and prevention.

## Scope

This policy applies to all lab computers, faculty computers and other staff computers that are PC-based or utilize PC-file directory sharing and Internet. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

## Policy

All PC-based lab computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

## Appropriate Use of Recourses

The CGI is committed to ensuring a working and learning environment in which all persons treat others with humanity and respect. Institute information technology facilities include computing devices and associated peripherals, communications infrastructure and related equipment, facsimile machines, scanners, copiers, telephones, video and other multimedia devices and all forms of software.

Such resources and tools are made available to employees in support of their teaching, research, and administrative activities and to students in support of their respective academic objectives and requirements.

Every users bears primary responsibility for the material he or she chooses to access, store, print, send, display or make available to others. The facilities may not be used in any manner to create, store, send, display or make available to others material which contravenes the relevant policies or statutes. When devices, such as portable

computers, are the property of the user, the appropriate use expectations still apply when such devices are used to access Institute information technology facilities.

Failure to adhere to these guidelines may result in the suspension of access privileges as well as other action as deemed appropriate by the user's division, CGI Computing and Networking Services.

Appropriate use of information technology includes, for example:

- respect for the rights of others
- respect for the property of others
- consideration of other persons using shared systems, equipment and facilities
- confidentiality in use of passwords and personal identification numbers
- a presumption of the right to privacy
- use of tools for the purpose for which they are intended
- adherence to the rules governing use of accounts, equipment, networks, or other facilities, whether the rules are established by the CGI or by the organization providing these tools to the Institute, and
- adherence to etiquette and culture as defined in systems that you use

Inappropriate use of information technology includes, for example:

- unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software, or systems
- deliberate over-extension of the resources of a system or interference with the processing of a system
- disclosure of confidential passwords, personal identification numbers and/or access devices or information for accounts, equipment, and telephone voice mail
- use of Institute facilities and resources for commercial purposes
- propagation of hate literature
- propagation of pornographic materials
- harassment, including sexual harassment
- theft of resources
- malicious or unethical use, and
- use that violates provincial or federal laws

## Personal Privacy

The property of the Institute includes the facilities related to computing accounts and files and other aspects of the information technology network in a similar manner to the telephones, filing cabinets, desks, etc., which an employee uses in carrying out the duties of her or his job. In principle, they are subject to inspection at any time. In

practice, however, such inspections other than for verification of physical assets are unusual and take place only where there is reason to suspect an infraction of the rules.

Generally, with respect to computing accounts established for students, faculty and staff there is a presumption of privacy. Under certain circumstances, access to files is authorized by Institute policy, or, for example, certain student files may be accessed by instructors as part of course requirements. However, if an infraction is suspected, the appropriate officials at the CGI will investigate the matter and, if circumstances warrant, proceed to investigate the traffic and files associated with the suspected infraction in accordance with the applicable Institute policy or procedure.

Such action requires the authorization of the respective chair or department head and/or dean or principal or vice-president. The Director, Computing and Networking Services should be advised promptly of any such action and that office is available to provide technical advice and guidance regarding suspected occurrences of inappropriate use. Local units are encouraged to establish, through a standing order from the appropriate academic or administrative head, the range of actions available to the designated individuals with responsibility for oversight of local information technology facilities.

It is essential that all users of information technology facilities and services recognize that it is possible for unauthorized individuals to monitor transmissions on networks in certain circumstances. It is also possible, for example, to create and send counterfeit mail under the name of another person and in a manner which makes it appear the message has emanated from the named user's desktop. It is suggested, therefore, that confidential information not be sent electronically unless the user is operating on a known secure network or is using encryption mechanisms.

## Network Security Policy

### Preamble

This document establishes the network security policy for the CGI .

The network security policy is intended to protect the integrity of campus networks and to mitigate the risks and losses associated with security threats to campus networks and network resources.

Like many other organizations, the CGI has experienced and will continue to experience security incidents encompassing a broad scope of severity. These incidents range from individual virus infections to loss of network connectivity for entire departmental zones

due to denial of service attacks. The management of these incidents is a responsibility of the Institute. Failure to meet that responsibility could result in a tarnished reputation as well as potential legal liability.

Attacks and security incidents constitute a risk to the Institute's academic mission. The loss or corruption of data or unauthorized disclosure of information on research and instructional computers, student records, and financial systems could greatly hinder the legitimate activities of Institute staff, faculty and students. The Institute also has a legal responsibility to secure its computers and networks from misuse. Failure to exercise due diligence may lead to financial liability for damage done by persons accessing the network from or through the Institute. Moreover, an unprotected Institute network open to abuse might be shunned by parts of the larger network community. This policy will allow the CGI to handle network security effectively.

This policy is subject to revision and will be evaluated as the Institute gains experience with this policy. All revisions are reviewed and approved by the Technical Operations Committee. Procedures and guidelines associated with this policy will be posted on the Computer Security Administration web page.

## Goals

The goals of this network security policy are:

- To establish Institute wide policies to protect the Institute's networks and computer systems from abuse and inappropriate use.
- To establish mechanisms that will aid in the identification and prevention of abuse of Institute networks and computer systems.
- To provide an effective mechanism for responding to external complaints and queries about real or perceived abuses of Institute networks and computer systems.
- To establish mechanisms that will protect the reputation of the Institute and will allow the Institute to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to the worldwide Internet.
- To establish mechanisms that will support the goals of other existing policies, e.g.
  - **Appropriate Use of Information Technology**
  - **Student Code of Conduct**

Note: Any violation of the network security policy will also be deemed a violation of the above listed policies, as appropriate.

## Policy Statement

The CGI provides network resources to its divisions, faculties and departments in support of its Academic Mission. This policy puts in place measures to prevent or at least minimize the number of security incidents on the campus network without impacting the academic mission or the integrity of the Institute's many different computing communities.

The responsibility for the security of the Institute's computing resources rests with the system administrators who manage those resources. Computing & Networking Services (CNS) and the Computer Security Administration (CSA) group will help system administrators to carry out these responsibilities according to this policy.

The Provost has overall responsibility for this policy.

The Technical Operations Committee of the Computer Management Board will review and respond to formal complaints resulting from the implementation of this policy. Computing & Networking Services (CNS) will prepare an annual report for the Committee relating experience with this policy and the Committee will recommend improvements to the Provost.

Departments, which administer LANs connected to the backbone, will:

- Provide Computing & Networking Services (CNS) with the names, email addresses and telephone numbers for at least two different contacts: a management contact; and a primary technical contact (usually the System Administrator). An alternate contact should be provided in situations where both the management contact and the primary technical contact are one and the same person.
- Assign to an individual, the authority to connect systems to the departmental network(s).
- Ensure this information is kept accurate and up to date.

Computing & Networking Services will:

- Monitor in real-time, backbone network traffic, as necessary and appropriate, for the detection of unauthorized activity, intrusion attempts and compromised equipment.

- Such monitoring will be carried out in compliance with the Institute's statement on Personal Privacy in the Appropriate Use of Information Technology;
- When a security problem (or potential security problem) is identified CNS will seek the co-operation of the appropriate contacts for the systems and networks involved in order to resolve such problems, but in the absence or unavailability of such individuals may need to act unilaterally to contain the problem, up to and including temporary isolation of systems or devices from the network, and notify the responsible system administrator when this is done;
- Carry out and review the results of automated network-based vulnerability, compromise assessment and guideline compliance scans of the systems and devices on Institute networks in order to detect known vulnerabilities, compromised hosts, and guideline compliance failures,
  - CNS will inform the departmental system administrators of planned scans activity providing detailed information about the scans, including time of scan, originating machine, and test and vulnerabilities tested for. The security, operation or functionality of the scanned machines should not be endangered by the scan;
  - If identified security vulnerabilities, compromises or guideline compliance failures deemed to be a significant risk to others and which have been reported to the relevant system administrators, are not addressed in a timely manner, CNS may take steps to disable network access to those systems and/or devices until the problems have been rectified.
- Prepare recommendations and guidelines for network and system administrators, to be posted at the Computer Security Administration Web Page,
- Provide assistance and advice to system administrators to the extent possible with available resources,
- Issue semi-annual requests to verify the accuracy of departmental contact information.

The Computer Security Administration group within CNS will:

- Co-ordinate all CNS network security efforts and act as the primary administrative contact for all related activities,
- Co-ordinate investigations into any alleged computer or network security compromises, incidents and/or problems. To ensure that this co-ordination is effective, security compromises should be reported to Computer Security Administration - Email: [itsupport@theciis.org](mailto:itsupport@theciis.org)
- Co-operate in the identification and prosecution of activities contrary to Institute policies and the law. Actions will be taken in accordance with relevant Institute Policies, Codes and Procedures with, as appropriate, the involvement of the Campus Police and/or other law enforcement agencies,

- In consultation with system administrators, develop procedures for handling and tracking a suspected intrusion, and deploy those procedures in the resolution of security incidents.

System Administrators will:

- Protect the networks and systems for which they are responsible,
- Employ CNS recommended practice and guidelines where appropriate and practical,
- Co-operate with CNS in addressing security problems identified by network monitoring,
- Address security vulnerabilities identified by CNS scans deemed to be a significant risk to others,
- Report significant computer security compromises to Computer Security Administration.

Network users will:

- Abide by the Appropriate Use of Information Technology policy of the Institute,
- Abide by departmental policies governing connection to departmental networks.

## Definitions

Network Resources	Network resources include any networks connected to the CGI backbone, any devices attached to these networks and any services made available over these networks. Devices and services include network servers, peripheral equipment, workstations and personal computers (PCs), etc.
CSA	Computer Security Administration
Departments	Department is used as a generic term to signify an academic or administration unit.
CNS System Administrator	Computing & Networking Services Refers to the individual who is responsible for system and network support for computing devices in a local computing group. In some instances, this may be a single person while in others, several individuals some of whom may be at different organizational levels may share the responsibility.

## Staff and Student Policy

### 1. Usernames and Passwords :

Window logon Usernames and Passwords are assigned to all the students, faculty and staff. Username for your Window Login Account for students is, their enrolment no assigned to them, and for faculty and staff it is by their names. The initial password is "CGI123". For example, the complete login username and password for student being enrolled to a course, with enrolment no. as course07002:

Username: course07002

Password:CGI123

### Computer Account :

A computer account is created for all full students and all the staff. You must login to this account anytime you use a college computer. See the section on Usernames and Passwords above for login procedures. The first time you login to the computer you will be asked to change your password. YOU MUST DO THIS. Your new password should be at least 5 characters long. Your password must be different than any that you have used previously.

---

### 2. Protect your Data :

You have been assigned 200 MB of storage space on the Z: Drive. B this is a secure storage area on the Network and is accessible only by you. We suggest you use the space to save your assignments. When you no longer need your assignments please delete them to free up the space. We suggest saving the latest version of your files on the Z: drive, and a backup of your files on a pen drives or " floppy disk".

Transfer files from home to the college or college to home by e-mail, as an attachment, to avoid corrupted floppy disks.

The college uses Microsoft Office 2000/XP Suite exclusively. If you use another product elsewhere, convert the file(s) to a Microsoft Office format before you bring your disk to the college to open or print the file(s).

---

### 3. E-Mail / Web mail Account:

Horde is the college's staff and faculty email system. You can access Horde through a web browser both on and off campus. Microsoft Internet Explorer (ver 4.0 or higher) is preferred, but Netscape Communicator and Mozilla also work. Set your browser to the Location <http://webmail.theciis.org>

See the section on [Usernames and Passwords](#) for login procedures.

NOTE: When you must change your password after getting the account activated by the System Administrator to avoid misuse of your accounts.

#### 4. SECURITY PROCEDURES FOR COMPUTER USE :

All information stored on a computer should be treated with the same sensitivity as paper files. Staff is responsible, not only for ensuring that information is protected from unauthorized use but also for the safety (i.e. backups and storage) of electronically stored data.

##### General Guidelines:

Staff should not leave their microcomputer or terminal with "work in progress" on the screen. This can lead to accidental loss or damage to that file or data. This is particularly important if confidential data is displayed on the screen.

It is recommended that staff regularly (e.g. every 10 to 15 minutes) save files or documents which they are creating so that as little work as possible is lost due to power outages or machine failures.

To protect office files from computer viruses disks used on home computers, which use non-standard or 'free' software should not be brought into the office.

##### Treatment of Confidential Files

Confidential files should never be stored on a microcomputer hard drive, a network drive.

Whenever possible delete confidential documents after printing.

Confidential documents, which must be kept in digital format, should be stored on floppy disks. The disks should then be locked in a secure, non-portable cabinet.

##### Backup Guidelines:

Files created or updated on the on administrative networks are backed up regularly by Computer Services or by the administrative department responsible for the network. All other users are responsible for their own backups.

Backup and recovery plans should be approached on an office wide basis so that files can be recovered even in the absence of a key person.

Network Security:

Staff should never give their network login password to another person.

Staff is personally responsible for any errors or damage that may occur under their username(s).

Staff should never use another person's login privileges on a network login.

Supervisors whose staff use the computer network login are responsible for notifying Computer Services if staff leave the college or are reassigned to other duties.

All computer users should report any operation abnormalities to Computer Services so that they may check for security breaches, viruses, etc. before the damage spreads.

---

#### 5. Computer and Internet Use in Library Policy:

CGI Library computers and computer resources are provided for the use of CGI students, faculty and staff to support study, research and teaching. Library patrons may use the Library's PC workstations to:

- Search the library catalogue, online or CD-ROM databases, and the internet
- Capture search results to print, save to disk, or save to an e-mail account

Users of the library computers are not permitted to:

- Enter chat rooms.
- Use word processing and other applications not loaded on library computers
- Play interactive games
- Conduct private business or engage in commercial activities
- Modify or reconfigure hardware or software

The use of library PC workstations, databases and Internet resources is subject to CGI policies with respect to copyright, privacy, harassment and student discipline. In order to preserve the integrity of the Library's computer resources against damage, failures or improper use, CGI Library reserves the right to limit, restrict or terminate any user's access to the Library computers.

## Wi-Fi Use Policy

Continental Institute for International Studies offer wireless access to the internet via the CGI Wi-Fi network. This WI-FI service is available to students and staff, who brings their own properly configured equipment to the WI-FI service area in CGI Jalvehra Campus. WI-FI is a public service to Students and Staff of CGI at free of charge, subject to the following terms and conditions.

Terms of use:

Use of the wireless network constitutes an agreement to be bound by the terms of the CGI WI-FI Internet Use Policy. Please read the policy before using the service. Failure to comply with the policy guidelines can lead to loss of network access, suspension of privileges, and/or prosecution. Users of CGI WI-FI agree to be monitored.

Please be advised that:

Continental Institute for International Studies is not responsible for insuring the privacy of information you transfer over CGI WI-FI. Virus and security protection is the user's responsibility. Information passing through the CGI Wi-Fi network is not secured and could be monitored, captured, or altered by others.

It is Sole responsibility of User (Students or Staff) to register their Wireless equipment with IT Deptt. of CGI, for using CGI WI-FI Network. Users will be provided IP Address for particular Wireless Device. It is sole responsibility of user to prevent the malicious use of their IP Address by someone else.

Continental Institute for International Studies assume no responsibility for damage, theft, or loss of a customer's equipment, software, data files or other personal property brought into or used on the CGI Wi-Fi network.

Continental Institute for International Studies will not provide technical assistance. There is no Help Desk facility.

There is no guarantee that you will have wireless access via the CGI Wi-Fi network at any specific time, location or with any specific equipment. Service disruptions may occur, and some equipment may not be compatible. Wireless access is provided as a public service free of charge on an "as is" basis with no guarantee and no warranty.

There is no guarantee that you will have access to every Internet site using the CGI WI-FI connection.

## Limitations & Disclaimers

It is the users sole responsibility to protect their information from all risks associated with using the Internet, including any damage, loss, or theft that may occur as a result of such use of SS WI-FI.

Continental Institute for International Studies will not provide technical assistance and assume no responsibility for laptop configurations, security or changes to data files resulting from connection to the CGI Wi-Fi network.

In using this free Internet access, I agree and hereby release, indemnify, and hold harmless, Continental Institute for International Studies, its officers and employees, and any affiliate, from any damage that may result in my use of CGI WI-FI.

While using CGI WI-FI, I acknowledge that I am subject to, and agree to abide by all laws, and all rules and regulations of the Cyber Law of India, and the federal government that are applicable to Internet use.

At its sole discretion, Continental Institute for International Studies may terminate CGI WI-FI at anytime without prior notice.

Printing is not available via the wireless connection.