THE GRADUATE INSTITUTE GENEVA

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

Terms and Conditions for Use of the Institute's IT Resources

1. Conditions of use, objective and scope

1.1. Conditions of use

The use of the IT (for Information Technology) resources of the Institute is provided at the discretion of the latter. This use does not confer upon users any vested rights. The Institute can choose to restrict or withdraw all or part of the use granted, without prior notice and without compensation.

1.2. Objective

The current Terms and Conditions for Use of the Institute IT Resources (hereafter "Terms and conditions") seek to fix the framework for use and protect the interests of the Institute and the user in the area of oversight of IT resources.

1.3. Scope

These Terms and Conditions apply to everyone who can access any IT resource: registered candidate, internal or external student, alumnus, participant to Executive Education programmes, internal or external collaborator, affiliated person, visitor, consultant (hereafter designated by the single term "user").

IT resources include all equipment and services related to the field of IT (including derivative applications) and made available to the user by the Institute, regardless of place of use and/or type of access (on-site, remote access, by cable or wireless, etc.).

The use of the Institute's IT resources by the user implies the full acceptance, by the latter, of all the clauses of the current Terms and Conditions and any related clauses and conditions arising therefrom.

2. Interests and risks for the Institute and the user

2.1. Interests and risks for the Institute

The use, at the Institute, of an equipment connected to a network (on-site or remotely) can pose a threat to the integrity of certain interests and technical equipment of the Institute. In particular, the following may be affected:
- the file storage capacity and the bandwidth, as a result, for example, of excessive use of the Internet or electronic mail;

- the security of the data and applications (availability, integrity, confidentiality), as a result of infections by viruses, worms, Trojan horses or the installation of software external to the Institute on the computers of the Institute;
- financial interests (increase in costs for supplementary equipment and/or services, network costs, etc.);
- other interests of the Institute protected by the law, including but not restricted to its reputation, or the confidentiality of data.

2.2. Interests and risks for the user

The interests of the user, particularly related to Internet surfing and e-mail as part of his activities at the Institute (information and communication), may be threatened in particular with regard to data protection or finance.

3. Measures for technical protection and journaling

3.1. Measures for technical protection

The Institute has implemented the following measures to protect its technical integrity:
- Secure access to the premises housing the data servers;
- User authentication through the use of confidential passwords;
- Protection against unauthorised access (access rights) to data or objects necessitating protection;
- Daily secure backup of files and management of disk quotas;
- Firewall to protect data from external attack;
- Anti-virus software to identify, and generally destroy, viruses and analogous elements.

The above mentioned measures can be adapted and updated with the development of new technologies.

3.2. Journaling

Most of the activities carried out using the Institute's IT resources are subject to journaling in log files. Journaling is the continual recording of "who, what, when" data. At the Institute, journaling is carried out in the following areas:
- On all the computers, operating systems (files and programmes used), and Internet browsers (history and cookies). The logging of this information is intended to improve the response times of applications. It is stored temporarily (in the cache).
- On the Institute's servers. Information is logged in order to control and ensure the optimum operation of the servers. The log files are not stored for more than one month;
- On the inter-site connecting equipment (firewalls, routers, switches, etc.). Journals are intended to control and ensure the optimum running of the network and management of the bandwidth. The logs are stored for no more than three months.

4. Rules of use

The IT resources are made available for professional and academic use. Personal use is tolerated within reason and according to the rules for use issued by the Institute. All abusive use and usage in breach of the law or that runs contrary to accepted mores is strictly prohibited.

The Institute's computers include a host of pre-installed applications and software. In order to avoid all risk of deterioration of computer content, all new software installation must be carried out by the IT Services of the Institute.

The rules for practical use are contained in a separate dedicated document[1].
In addition, collaborators are subject to the clause #8 of the Institute Internal Regulations[2].

5. Surveillance regulations

5.1. Priority for measures designed for technical protection

The Institute undertakes to give priority to measures designed for technical protection to prevent abuse and damage of a technical nature. It regularly updates the technical protection measures in line with technological developments. These measures are also updated following a technical breakdown. It is only authorised to carry out a nominative analysis of the data in the event that technical protection measures are insufficient to prevent abuse. It does not use any spy software.

5.2. Analysis of log files

The Institute may undertake anonymous or pseudonymous analyses of log files with a view to ensuring that the rules for usage are being respected. Anonymous analysis involves a statistical analysis of the log files and is used to check for items such as the most frequently consulted web pages. Pseudonymous analyses are carried out by survey only. Anonymous and pseudonymous analyses use a sufficient sample of data to guarantee confidentiality.

In the event that the Institute identifies an incidence of abuse during an anonymous or pseudonymous analysis, or any analysis that gives reason to believe that abuse has taken place, it will carry out a nominative analysis of the log files. All violations of the Rules of Use are considered to be abuse. In the event that abuse is deemed to have occurred, the Institute can choose to issue a punishment in line with Item 5.4 of the current Terms and Conditions. If the suspicion turns out to be unfounded, the Institute will cease all nominative analysis with immediate effect.

If the analysis of the log files or other facts reveals the existence of a crime or gives reason to suspect that abuse may be taking place, the Institute will retain the log files in question. It reserves the right to open proceedings against the user involved. Further action falls under the remit of the legal authorities. The Institute undertakes to keep the results of the inquiry confidential and to not divulge them to unauthorised third parties (including collaborators and students of the Institute). The decision about whether or not to pursue criminal proceedings is that of Management alone (or of any individual to whom it has delegated authority).

[1] Rules and Best Practice Guidelines for the Use of Information Technology Resources
[2] Règlement interne de l'Institut de hautes études internationales et du développement

5.3. Surveillance in order to guarantee the security and optimum functioning of the IT system or on the basis of other criteria

In the event that the Institute or a technical partner (Internet Service Provider, etc.) observes a malfunction of the IT system despite the technical protection systems in place, the Institute may proceed with an analysis of the journals to determine the cause. If the malfunction is imputable to abuse, the guilty user can be subject to punishment as outlined in Item 5.4 of the present document.
In the event that the Institute observes abuse or believes that abuse has occurred because other indicators give reason to believe this, it may consult the relevant log files and their analyses. In the event that abuse has taken place, it can choose to apply one of the punishments outlined in Item 5.4 of the current document.

5.4. Punishment for abuse

If the necessary conditions for surveillance and the rules governing the same have been appropriately applied, the Institute may, if it observes abuse, take punitive action against the offending user. Possible punishment will be decided by Management.

5.5. User rights in relation to abusive surveillance

In the event that the necessary conditions required for surveillance and the rules governing their implementation are not respected, the user may invoke the provisions foreseen for this purpose by the Civil or Criminal Codes.

5.6. Other dispositions

IT Services and the Management of the Institute establish all the technical measures necessary to prevent the personal data they are investigating during the surveillance process coming into the possession of unauthorised persons. In particular they will take all the measures necessary to protect the confidentiality, availability and integrity of these data.
The user may at all times ask the Institute if data concerning him/her are subject to surveillance, and if so, which data.
Personal data cannot be communicated to unauthorised third parties without a valid motive and in the absence of the agreement of the individual concerned.

6. Responsibilities and limits of responsibility

6.1. Scope of user responsibility

As a general rule, the user is responsible for all damage resulting from non-regulatory use of IT resources.
In particular, the user will be held personally responsible for

- The implementation of IT security corresponding to the end-user level
- The safety and integrity of all the data with which s/he is dealing
- All actions carried out in the name of his/her account
- All information s/he makes available to third parties
- All damage and punishments resulting from the failure to respect legal or regulatory dispositions, including third party intellectual property rights (for e.g., failure to respect software licences, etc.).

6.2. Scope of the Institute's responsibility

The Institute endeavours to put in place, within reason, all technical measures, technology permitting, to ensure the availability of effective, functioning IT resources; however, the Institute declines all responsibility for damage incurred, regardless of the nature (direct, indirect, etc.), from the use of its IT resources.

The Institute also employs all reasonable facilities, technology permitting, to guarantee the safety of the IT resources; however, the Institute provides no guarantee of any sort regarding the safety and accuracy of the IT resources made available, and, declines all responsibility to this effect, in line with the conditions stipulated in the previous paragraph.

7. Entry into force

The current Terms and Conditions enter into force as of September 2nd 2009

The French-language version of this document is the authentic text.

8. Updates

V120 – 24.08.2015: scope extension to include participants to Executive Education programmes
V200 – 22.06.2017: scope extension to include all users of IT resources at the Institute. New document name where "Notice" is replaced by "Terms and Conditions".