THE GRADUATE INSTITUTE GENEVA

INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT

GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES

Rules and Best Practice Guidelines for the Use of Information Technology Resources

You have been assigned an Information Technology Account (hereafter IHEID IT Login) to enable you to access the different Information Technology (hereafter IT) resources available at the Institute. If necessary, you have also been assigned an email account (hereafter IHEID Email Login), linked to an email address (firstname.name@graduateinstitute.ch).

The use of the above mentioned accounts is subject to the current rules and best practice guidelines[1] derived from the Notice for Use of Information Technology Resources of the Institute ("Notice").

The IHEID IT Login and IHEID Email Login credentials are confidentially transmitted.

The current document applies to students, employees and Executive Education participants of the Institute, as defined in the Notice. Students, employees and participants will hereafter be designated by the single term "user".

1. Utilisation of IT Resources

1.1. Duration of access to IT resources

Your IHEID IT Login and IHEID Email Login, if you have one, are valid for the duration of your studies at the Institute, your contract of employment, your mandate or your stay at the Institute.

1.2. Framework governing use

1.2.1. For students

Students are requested to restrict their use of the available resources to academic purposes related to their studies.

1.2.2. For employees

Employees are requested to restrict their use of the available resources to professional purposes related to the execution of their jobs.

1.2.3. Limited private use

Limited private use of the IT resources of the Institute is tolerated subject to certain conditions and providing,

a) It does not contravene legal or regulatory provisions (cf. on this subject items 1.7 and 2.7, below);

[1] Management and the IT Service may amend these user rules if required. Users will be informed through the publication of new rules

b) It is for non-profit activities and non-propaganda purposes;
c) It is not likely to prejudice the Institute in any way, in particular as concerns its reputation and image;
d) There is no confusion between the nature of the private use and use by the Institute, in particular, provided it does not engage the latter's responsibility;
e) It is compatible with the interests of the Institute and the values promoted by the latter;
f) It does not result in excessive consumption of IT resources (network, storage, etc.).

In keeping with this, when using Institute resources for private purposes, users will take all the necessary measures to ensure, in particular that

a) Their electronic addresses provided by the Institute do not appear on documents unrelated to their studies or unrelated to their duties at the Institute (for e.g., documents produced for propaganda purposes, etc.);
b) No signature pads implicating the Institute figure in their private electronic mail;
c) That no single e-mail message is used for both academic/professional purposes and private purposes (two separate e-mail messages should be sent, one for each purpose);
d) That the sender's first name and name appear clearly in the message.

1.3. Login to an Institute computer

In order to work on one of the Institute-owned computers, users are required to identify themselves using their IHEID IT user name and password. To login to PCs, users must type the user name and password given to them upon arrival at the Institute.

1.4. Protection of the infrastructure

None of the Institute equipment connected to the IT network may be unplugged or moved, irrespective of the type of connection (cable, wireless, etc.). No equipment external to the Institute may be connected to the network via a cable.

1.5. Protection of software licences

It is strictly forbidden to copy licensed software or software provided by the Institute. Indeed, copying software is illegal if it is not free or open access. We draw the attention of users to the legal consequences of violation of intellectual property rights and copyright law (LDA). All software put at the disposal of users is subject to legal and contractual provisions.

1.6. Limits of Internet usage

The use of peer-to-peer software programmes is prohibited. Indeed, they slow down the technical performance of the IT installations and are frequently in contravention of copyright law.

1.7. Legal framework for use

Users must ensure that they respect third party rights so as not to infringe civil, and in some instances, criminal law.
It should be remembered that users can be subject to civil and/or criminal proceedings not only if they commit an illegal act, but if they are implicated as co-authors, accomplices or instigators of such actions.

1.7.1. Civil law (e.g., copyright law, logos and trademarks, data protection)

It is strictly prohibited to disseminate, including on the web, works or extracts of works that are protected by copyright law, except when expressly permitted by the law (prior consent of the author, etc.). The following are in principle protected by copyright law: scientific works, literary works, computer programmes, images, music, songs, videos, etc.

It is strictly prohibited to use logos and trademarks belonging to third parties, especially for the purposes of offering products and services identical or similar to those for which the trademarks or logos have been registered. These elements can be quoted in an editorial context provided that it does not infringe the restrictions previously stated.

It is strictly prohibited to disseminate, including on the web, third party personal data such as information on political or religious opinions, religious affiliation or other information related to the personal sphere without the prior and explicit consent of the individual concerned.

1.7.2. Criminal law

The use of IT resources must not contravene the dispositions of the Swiss Criminal Code and/or the criminal components of specific applicable laws (e.g., copyright law). This provision is applicable not only to IT offenses, but also to all offenses that can be committed electronically.

In particular, users are prohibited from creating, concealing, possessing, searching, posting, accessing without permission or disseminating elements which contravene the moral standards, dignity of the individual, the Institute or its members and/or which constitute a personal attack (defamation, libel, etc.), acts which amount to racial discrimination or which are in breach of sexual integrity (pornography, etc.).

2. Security

2.1. User responsibility

All IHEID IT Logins and IHEID Email Logins are personal and password protected. Users are responsible for all actions carried out in the name of their user account. Therefore, it is strictly prohibited to communicate passwords to a third party for whatever motive. In particular, confidential information must never be communicated by email in response to messages seeking to obtain or steal identity (phishing). In the event of any doubts, an e-mail message should be sent to servicedesk@graduateinstitute.ch.

2.2. Protecting the work session

Users are advised to lock their work session even during short absences from the workstation (e.g., lunch). Users must log off from the workstation during absences of several hours or at the end of the working day.

2.3. Secure storage space

All PC workstations offer secure storage space on the server. This space is based on an allocated quota. Users must ensure that they do not exceed these quotas failing which data.

Outside this secure space, users are responsible at all times for regularly saving their work in sufficient copies and in different places.

2.4. Saving data

In the event of a breakdown or change of computer it will not be possible to retrieve data stored in areas other than the secure storage space. In the event of loss, only data saved on the server, which is backed-up each day, can be retrieved.

2.5. Data protection

Users should refrain from opening .zip files unless they are 100% sure of their provenance. Data are exposed to the dangers of viruses hidden primarily in email attachments, USB sticks and transmitted via the Internet.

2.6. Conserving workstation integrity

All new software must be installed by or in collaboration with the IT Service. The integrity of the user workstation will depend on the software installed.
All action aimed at by-passing or deactivating the security systems (software and hardware) is strictly prohibited.

2.7. Legal security framework

The legal framework for security is governed by the Swiss Criminal Code[2]: cf. for e.g., art. 143 (concealment of data), 143bis (unauthorised access to an IT system), 144 (damage to property), 144bis (deterioration of data), 147 (fraudulent use of a computer), 150 (fraudulent acquisition of a service).

3. Surveillance and punishment

Paragraph 5 of the Notice lists the principles governing monitoring and surveillance and the punishment to which users in breach of these conditions are exposed. In the event of a failure to respect the legal or regulatory framework, user access can be terminated without prior notice.

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

[2] http://www.admin.ch/ch/f/rs/c311_0.html