Rules governing the use of Information and Communication Technology (ICT) hardware by contractors

Article 1
This document applies to individuals who, in connection with the execution of a service or works contract between (i) Electrabel or another ENGIE Group company (hereinafter "the Client") and (ii) a contractor (hereinafter "the Contractor"), have been entrusted with Information and Communication technology hardware (hereinafter "ICT hardware") by the Client. These individuals are hereinafter referred to as "Users".

The Contractor is responsible to the Client for ensuring that its personnel comply with the obligations set out in this document. The Contractor undertakes to have its personnel read this document prior to using any of the Client's ICT hardware and to require compliance herewith.

Article 2
The ICT hardware must be exclusively used with the installed official software and hardware (developed for the Client, purchased or leased under licence).

Permission to install a programme that is not part of the standard package on the ICT hardware provided by the Client (PC, PDA, etc.) must be expressly sought from the Client's Information Security Manager (ISM).

Article 3
Each user must take the required measures to prevent the theft of the ICT hardware provided to him by the Client. The Client is responsible for the mechanisms for protecting IT hardware.

Article 4
The User must use the hardware prudently and diligently and such use may not jeopardise the smooth operation of the Client's company, nor may it adversely impact on the image and reputation of the Client in respect of third parties.

Article 5
The Client attributes a password and user ID to each User. The password must be formed in accordance with the rules defined in the Password Policy accessible via the Client's intranet.

Article 6
The user ID enables the User to be clearly identified by the IT systems.

The password is personal and may not be divulged to anyone.

Article 7
Any User having access to the Client's IT system, regardless of its form, is responsible for the use he makes of said system.

Article 8
When sending e-mails, Users must systematically sign the message on behalf of their employer/organisation, as follows:

User's first name and last name
Name of the User's organisation/employer, contractor of Client

f.i.:
Jean Dupont
Bullax s.a., contractor of Electrabel s.a.

The User is not authorised to send e-mails on behalf of another User, unless the latter has expressly authorised the former to do so.

Using another User's password and login is strictly forbidden.

No exceptions to these rules are allowed except with the prior written authorisation of the Client's authorised Information Security Manager (ISM).

Article 9
IT applications may not be left unsupervised for an extended period without blocking access to the applications (Control-Alt-Delete / Lock computer).

Article 10
E-mails sent within the Client's company are confidential and may not be forwarded to addresses outside the Client's company or to other Users, unless required for purposes relating to the provision of services and the recipient can be considered an authorised individual. Any e-mail containing confidential information must be designated as such.

The sending of highly confidential messages by e-mail should be avoided, except when sufficient security measures have been taken.

Article 11
Incoming e-mails are systematically checked for viruses. Any message containing a virus will be automatically deleted. The sender and recipient will be informed of this via a special notification.

Article 12
A disclaimer must be added at the bottom of e-mails sent to addresses outside the Client's company. The disclaimer will automatically be added to all outgoing e-mails.

Article 13
Users are not authorised to automatically forward e-mails to their private address (specifically by activating the option of automatically redirecting incoming e-mails), even during periods of absence (during periods of leave, for instance). In the latter case, Users are advised to use an "Out of Office" message in which they indicate the name of the Contractor staff member who will be temporarily carrying out their duties during their absence, where appropriate.

Article 14
Users may not be held responsible for messages they receive, provided they did not solicit those messages. However, if a User sends messages that run counter to the provisions of this document to one and the same person on multiple occasions, then the User in question must take adequate measures to put an end to the sending of such messages (either by clarifying the matter with the author of the messages, or by informing the Client's Information Security Manager) or inform the employer, which must then examine the appropriate measures with the Client.

Article 15
The Client has installed software that filters the content of websites that Users wish to access. This filter makes it possible to block access to websites whose content is deemed illegal, offensive or inappropriate. Accordingly, the Client has blocked access to all sites falling within certain categories, such as pornography, nudity, online games, MP3 files, chats or instant messaging. When Users try to access one of these sites, they receive a message informing them that access is blocked and stating the category to which the site belongs.

Any problem relating to the Internet filter – i.e., when a User needs to nevertheless access a website for professional reasons – must be reported to the Client's Information Security Manager.

Article 16
The following are prohibited:

- Divulging confidential information about the Client, one or more Users, the Client's employees, the Client's clients or third parties, unless the dissemination of such information is duly justified by reasons of a professional nature;
- Attempting to access the e-mails of other Users or third parties in order to read them;
- Consulting, sending or keeping texts, images or audio recordings of a racist, erotic, pornographic, sexual or obscene nature, or having a comparable content, regardless of the origin of such texts, images or audio recordings (e.g., USB port, CD, DVD, etc.).

Article 17
Sending messages to large groups (more than 100 individuals) without the prior written express authorisation of the Client's Information Security Manager is also prohibited.

Article 18
The sending and reception of long messages are automatically limited in order to prevent any risk to network availability. Any attachment to an incoming or outgoing e-mail sent via the Internet exceeding 25 MB and all incoming messages containing attached executable files will be deleted. Those Users who must be able to regularly send or receive messages whose size exceeds the indicated limit must contact the Client's IS Service Desk.

Article 19
Streaming is not authorised, except during the provision of services. Videoconferences are authorised. Screening and listening to work-related information are authorised. Using the ICT hardware to listen to radio stations and watch videos not related to the services provided is prohibited.

Article 20
Checks aim primarily to ensure respect for the privacy of the Users of ICT hardware and to define ahead of time the rules to be followed by the Client when the Client wishes to check electronic communications (Internet and e-mail).

All checks will be carried out in consideration of the following principles:

– **Objectives**: This document summarises exhaustively the objectives in connection with which a check may be organised.
– **Proportionality**: The check and its scope must be appropriate, pertinent and moderate in all cases. They must also be proportional to the defined objective(s), but must always be kept to a minimum.

– **Transparency**: The purpose of disseminating this document is to inform Users about the rights and obligations of each party.

Article 21
All checks will be carried out by the IS department, under the responsibility of the Client's Human Resources department or the Client's Chief Security Officer.

Article 22
If a breach of the provisions of this document is observed, the Client will communicate to the Contractor, the User's employer, all information required regarding the breaches, will be entitled to ask to the Contractor to undertake the necessary corrective actions, and may refuse to let the User in question use the ICT hardware, with immediate effect.

Article 23
Failure by a User to comply with the provisions of this document may also be considered a breach of contract by the Contractor, the User's employer, in connection with the execution of the service contract.

Article 24
Any User who notices an anomaly in the operation of the IT system must report it to the IS Service Desk or, in the event of security issues, to the Client's Information Security Manager (ISM).