GEWISS S.p.A.
IT CODE OF CONDUCT

Approved by the Board of Directors
on 25th July 2012

CONTENTS

INTRODUCTION

The progressive diffusion of new information technologies could expose GEWISS to both property and penal risks, creating in the meantime problems in corporate image and security, in case the information technology equipment is used in an incorrect way or for crimes.
The growing importance of confidential information within the company assets and the proper deriving competitive advantage for the company have made the same to equip itself with all suitable protection measures aimed at preventing the diffusion of confidential data and information which could both cause civil and penal liabilities for the person violating the company secrecy.
In confirmation of this fact and in compliance with the relevant European principles, the Italian legislator modified art. 99 of the Industrial Property Code and obliged the company wishing to protect its confidential information to be equipped with positive measures (for example security measures) for the protection of the confidential nature of information.
In particular, referring to the security measures as per Italian Legislative Decree n. 196 of 30th June 2003, about the processing of personal data, GEWISS has given suitable explanations and instructions to all "company users" who, working with information tools, are interested in the above mentioned measures.
Moreover, in compliance with the Legislative Decree n. 231 of 8th June 2001, GEWISS has drawn up its own Organization, Management and Control Model in order to prevent Directors, employees and third parties in general from committing crimes, as far as possible.
Considering that the use of corporate information and telematic resources must always be guided by care and fairness principles, attitudes that should always be taken while working, it is useful to adopt further internal behaviour rules within the information environment, directed to avoid unaware and/or incorrect behaviour.
This IT Code of Conduct replaces the one previously adopted by the Board of Directors on 19th March 2008.

1. DEFINITIONS

For the purpose of this IT Code of Conduct, the meaning supplied for each of the term and expression listed below is valid for the term/expression as follows:

- "**IT CODE OF CONDUCT**": this document;
- "**COMPANY**": the company *GEWISS* S.p.A.;
- "**SUPERVISORY BODY**": the controlling body pursuant to art. 6, lett. b) of the Legislative Decree 8th June 2001, n. 231;
- "**INFORMATION TECHNOLOGY EQUIPMENT**": any non-paper equipment used by each company user to carry out his/her tasks, among which, by way of an example, there are personal computers, both fixed or portable ones, PDA or smart phones, fixed and mobile telephones;
- "**INFORMATION SYSTEM**": resources, data, applications and programs on the IT equipment and/or data storage devices;
- "**COMPANY USER**": any user, even if he/she is not a COMPANY worker, who has been given one or more than one INFORMATION TECHNOLOGY EQUIPMENT and/or has been given access to use the company information system.

2. COMPANY INFORMATION SYSTEMS – GENERAL RULES

All INFORMATION EQUIPMENT, the respective programs and/or all applications, given to the COMPANY USERS are considered , as per art. 48 of the CCNL National Labour Agreement, as working tools. Therefore:

2.1 these tools must be kept in a proper way;

2.2 these tools could be used only for professional purposes (obviously related to one's duties) and not for personal aims, least of all for crimes;

2.3 it is forbidden to lend or give third parties any INFORMATION TECHNOLOGY EQUIPMENT, without the previous IT Director's authorization;

2.4 it is forbidden to remove the identification marks from the INFORMATION TECHNOLOGY EQUIPMENT;

2.5 any theft, damage or loss of computer equipment must be promptly reported to the *Corporate* Information & Telecommunications Department, to the Human Resources & Organization Department and to one's own Department. Moreover, if the computer equipment is stolen or lost, the person involved, or the person who was given the INFORMATION TECHNOLOGY EQUIPMENT of any kind, shall send the *Corporate* Information & Telecommunications Department the original copy of the report given to the Public Security Authority within 24 hours from the fact;

2.6 it is forbidden to introduce and/or keep within the COMPANY, by way of any capacity and for any reasons, (by means of any information tools, hardware and paper), all confidential and third party's I.T. material and/or documents, without the previous owner's authorization. It is understood that, in case of violation, the personal civil and penal liability of the employee as well as the COMPANY disciplinary sanctions shall be applied;

2.7 it is forbidden to bring out from the COMPANY and/or transmit files, documents, drawings, projects or any other COMPANY confidential documents, by means of computer, hardware and paper tools, if not for purposes strictly concerning the execution of one's task and, in any case, subject to the relevant Department Manager's authorization;

2.8 it is absolutely forbidden to share in common areas (such as, for example, Workspace/LAN folders etc.) or, in any case, to pass on documents and information within the company which are not linked to the sender or receiver's professional activities, by using any IT tools, hardware and paper;

2.9 it is forbidden the recording in the company INFORMATION SYSTEM of offensive and/or discriminating documents as to sex, language, religion, race, ethnic origin, opinion and trade-union membership and/or politics;

2.10 it is forbidden the recording of company documents in unauthorized storage devices (some examples are portable data storage devices, USB keys etc. are given as an indication);

2.11 in case of employment termination for whatever reason, the COMPANY USERS must give back to the *Corporate* Human Resources & Organization Department all INFORMATION TECHNOLOGY EQUIPMENT and the working tools assigned to them and at use conditions. Deletion of all data filed on the INFORMATION TECHNOLOGY EQUIPMENT and on working tools shall always occur in the presence of members of the *Corporate* Information & Telecommunications Department's staff;

2.12 at any time, the COMPANY has the right to differently use the INFORMATION TECHNOLOGY EQUIPMENT given to COMPANY USERS, to ask for its prompt return and/or to check it in order to verify its correct use.

3. USE OF INFORMATION TECHNOLOGY EQUIPMENT

To the above mentioned ends, every act or attitude contrasting with the previous instructions is forbidden. Some examples are given below as an indication:

3.1 To prevent the danger of a computer virus and damage to the stability of the personal computer and its applications, users are allowed to install external programs only when explicitly authorized by the Information Technology Director.

3.2 It is forbidden the installation and use of programs which are not authorized by the Information Technology Director who will give his/her authorization if the obligations as per Law n. 633 of 22nd April 1941 and subsequent modifications about the software legal protection and copyright are met.

3.3 It is forbidden to modify the configurations set on the INFORMATION TECHNOLOGY EQUIPMENT without the previous Information Technology Director's authorization.

3.4 It is forbidden to install on and/or connect to the INFORMATION TECHNOLOGY EQUIPMENT any additional peripheral devices which are not authorized by the Information Technology Director.

3.5 On PC equipped with audio devices and/or CD/DVD players, it is forbidden the listening to audio or music files or to watch videos and movies if not related to one's job.

3.6 Users are not allowed to leave their own INFORMATION TECHNOLOGY EQUIPMENT unattended and/or accessible to others. During long absence from work, the function Lock PC/equipment must be activated.

3.7 It is forbidden to leave any portable INFORMATION TECHNOLOGY EQUIPMENT (laptops, PDA, smart phones, video-projectors, cell phones, etc.) unattended and/or accessible to others during transfers (example parking areas etc.), business trips (example: airports, stations, etc), or, in case of absence from the COMPANY (holidays, on weekend, during the night).

4. PASSWORDS

4.1 Passwords giving access to the Company LAN must be kept secret pursuant to the Security Measures as per Leg. Dec. N° 196 dated 30th June 2003. Therefore everyone has to protect the secrecy of passwords.

4.2 Passwords must not be given to anyone. Labels and/or tickets reporting user-id and/or passwords cannot be exposed on the PC.

4.3 Passwords must be 8 characters long, they must not contain references to the user, they must be modified by the user himself/herself at first access and must be changed at least every three months.

4.4 It is absolutely forbidden to use passwords belonging to other COMPANY USERS, even if the access is to protected areas on behalf of the same COMPANY USERS, except when explicitly authorized by the COMPANY USER's Manager and the Privacy Owner.

5. USE OF THE COMPANY LAN

5.1 The network units and the Workspace area are shared areas containing strictly professional information and cannot be used for different aims.
The operational modes to correctly have access to electronic data are ruled in details in the Operating Instructions "I701 – Information Technology Privacy", which is an integral part of this document.
The COMPANY has the right to modify the access authorizations to the company LAN and to the relevant applications in case the integrity of all company information data is put at risk, even also potentially.

5.2 Any file which is not related to one's work cannot be placed, not even for short periods, on the COMPANY INFORMATION SYSTEM and on the INFORMATION TECHNOLOGY EQUIPMENT.

5.3 The access of each employee to any resource of the company INFORMATION SYSTEM (folders in the company LAN, shared areas etc.) must be authorized by the relevant Manager on the basis of the tasks assigned to each employee; each COMPANY USER must therefore use the company LAN for purposes strictly linked to his/her task, in compliance with what provided for by the authorization.

5.4 Each COMPANY USER has to protect the confidential nature of the data he/she is processing, by paying particular attention to shared data and to any paper copy of the electronic data and by removing them at once, when these data are no longer necessary; in particularly it is strongly recommended to password protect all documents which are temporarily filed in those shared areas which all COMPANY USERS can have access to.

5.5 At any moment the COMPANY has the right to remove any file or application considered as dangerous for the system security and any file or application acquired and/or installed violating the present IT Code of Conduct; in particular the COMPANY has the right to delete the data saved in shared areas common to all COMPANY USERS within 24 hours from their save.

5.6 It is forbidden to install and use software and/or hardware to intercept conversation (in any form it is, a phone conversation, a sms, e-mail etc.) and falsify, alter or suppress the contents of communications and /or company IT documents.

5.7 It is forbidden to connect to the company LAN any PC or other information technology devices not belonging to the COMPANY, except when explicitly authorized by the Information Technology Director.

6. USE OF INTERNET NETWORK AND RELATED SERVICES

The COMPANY guarantees, only to the COMPANY USERS who need it, the access to the Internet from their own workplace. The Internet connection must be kept for the time strictly necessary to carry out those activities linked to the use of the Internet. Therefore:

6.1 it is forbidden to surf sites not related to one's job;

6.2 it is forbidden to download and store unauthorized documents and insulting/discriminating documents as to sex, language, religion, race, ethnic origin, opinion, and trade-union membership and/or politics;

6.3 it is forbidden to execute any financial transaction included remote banking operations, on-line purchases and similar operations, except for those cases foreseen by the Company procedures ruling the company procurement;

6.4 it is forbidden to download from the Internet sites any type of software, if not explicitly authorized by the Information Technology Director;

6.5 it is forbidden any registration to sites whose content is not related to one's work;

6.6 it is forbidden to use and consult, for private reasons, services such as forums, social networks, chat-lines, newsgroup, electronic notice boards or similar and registration to guest books, even using nicknames;

6.7 it is forbidden to become a member of forums, chat-lines, blogs, newsletter or internet web sites linked to the working activity, using the company e-mail address, except when specifically and previously authorized by the relevant Department Manager. In any case, everybody is directly responsible for the correct and legitimate use of the company e-mail address, as well as of the content of the transmitted declarations and information;

6.8 the only authorized Internet connection is to the Company LAN; any other different connections, for example the ones using company phone lines, are therefore not authorized;

6.9 at any time, the COMPANY has the right to activate some filters on the Internet web surfing, by blocking the access to sites which are not linked to the working activity, to dangerous sites or sites which could potentially cause a violation of the Organization, Management and Control Model ("MODEL 231") adopted by the COMPANY.

7. USE OF ELECTRONIC MAIL

The COMPANY provides, to the extent of the COMPANY USERS who need it, a personal E-mail Box which is univocally assigned. Also the E-mail Box is a working tool available to accomplish the activities linked to the assigned tasks, therefore the address attributed to the COMPANY USERS is personal but not private. Everybody is directly liable, in front of the discipline and of the law, of the content of his/her own E-mail Box and of the sent messages. The management of these E-mail boxes is ruled in details by the procedure "P103 – E-mail Management", which is an integral part of this document.

It is also useful to underline that:

7.1 It is forbidden to use the electronic mail, both internal and external, for reasons not related to one's work;

7.2 It is forbidden to send or record any messages, internal or external of offensive and/or discriminating nature as to sex, language, religion, race, ethnic origin, opinion, and trade-union membership and/or politics;

7.3 All external messages, sent or received, by the Direction Secretary addresses are shared with the General Secretary;

7.4 Any external message, both sent or received, could be shared and seen within the COMPANY;

7.5 It is forbidden the use of electronic mail belonging to other COMPANY USERS to send messages in one's name or on behalf of the latter, except when there exists explicit authorization of the user himself/herself. In case of planned absence of the employee it is strongly recommended to the COMPANY USER to share his/her e-mail box, activating an automatic answer (the so-called "out of office" warning) with the possible indication of the reference people to be contacted in case of urgent matters and their electronic and/or phone references. The "Out of office" message must be activated both for internal and external senders;

7.6 The Direction Secretaries or Function Secretaries, as "FIDUCIARY", shall have access to the e-mail boxes of the absent COMPANY USERS and see all necessary messages in compliance with what provided for by the Laws about Privacy Protection and according to the instructions given in the specific procedure;

7.7 Personal e-mail boxes are created and assigned without any configuration for sharing and/or rules. Each COMPANY USER is therefore responsible for any possible sharing and/or rules applied on his/her Electronic Mail Box. Moreover rules as per paragraph 2.8 about document and information sharing on common areas shall also apply;

7.8 it is forbidden to create, consult, use private E-mail boxes;

7.9 the COMPANY has anyway made available some addresses shared by more than one COMPANY USERS, clearing up the non-confidential nature of the mails. These addresses generally correspond to service e-mail boxes or function e-mail boxes. All external communications, sent or received through these addresses shall be recorded.

8. CHECKS

8.1 In compliance with what provided for by Laws about Privacy protection and Labour, the COMPANY shall periodically check the company INFORMATION TECHNOLOGY EQUIPMENT assigned to users (cell phones included), their use and their related programs and/or applications, in order to detect any possible computer viruses and guarantee the integrity and security of the system, and to verify their correct use and to prevent any act or behaviour which could jeopardize the integrity of all company data.

8.2 In compliance with what provided for by Laws about Privacy protection and Labour, the COMPANY shall arrange specific, but not regular, checks on the use of the E-mail and Internet through the analysis of aggregated data in order to verify the correct use of the services and to prevent any possible behaviour which could jeopardize the integrity of all company data.

8.3 If an employee has the authorization to have access to certain information of the company INFORMATION SYSTEM, this authorization is be considered as strictly limited to the carrying out of one's task in line with the previously issued authorization forms. The COMPANY shall carry out specific, but not regular checks, on the COMPANY USERS' profiles, in order to verify the access to and management of the company data as well as the consistency among the assigned tasks, the given profile and the authorizations, finding out any behaviour which could put at risk the integrity of all company data.

8.4 The data analysed during those checks are not automatically nor systematically associated to identified COMPANY USERS, but because of their nature they could, by processing and associating them with other data, identify the COMPANY USERS.

8.5 In case a violation of the access authorization profiles to company data is ascertained, the COMPANY shall have the right to take all necessary measures to protect itself, considering these violations as serious non-fulfillment of law and of the employment contract.

8.6 The Internet data are used only in order to draw some statistical information about the use of the sites and also to periodically check their correct use, and they are kept for a limited time period.

8.7 All these data could be used for checking the liability in case of possible information crimes damaging the COMPANY as well as in case of litigations.

8.8 Any violation of this IT CODE OF CONDUCT can be sent to the e-mail address ia-odv@gewiss.com, as per what provided for by "Regulations regarding GW Spa reports" available on internet web site.

9. NON-OBSERVANCE OF INSTRUCTIONS AND SANCTIONS

9.1 The non-observance of the rules provided for by this IT CODE OF CONDUCT shall be the object of disciplinary evaluations applying sanctions such as warnings, fines, written cautions, work suspension up to three days and dismissal, also concerning the judiciary extent.

9.2 The COMPANY shall claim for compensation against the people responsible of possible damages deriving from a non conscientious or non conformable use of the rules written in this IT CODE OF CONDUCT.

9.3 As per Civil Code and per CCNL National Labour Agreement, the COMPANY USERS could be called to answer, also from a disciplinary point of view, in case of theft, loss and any possible damage to INFORMATION TECHNOLOGY EQUIPMENT due to a non conscientious use of the same; the relevant damages amount can be charged on the pay-sheet.