SPECIAL SECTION "H"

COMPUTER CRIMES AND ILLEGAL DATA PROCESSING

CRIMES RELATED TO THE INFRINGEMENT OF COPYRIGHT

CEO Approval Luigi Michi
04 December 2017

TABLE OF CONTENTS

DEFINITIONS

With the exception of the new definitions included in this Special Section "H", the definitions of the General Section remain valid.

Machine Administrator (AdM): assignee of a Computer Workstation with Local Administration Permissions.

Database Administrators, Network and Security Administrators and Program Administrators: such persons not system administrators but have advanced access permissions in relation to the activities carried out. Such persons are therefore equal to Machine Administrators in terms of data protection risks.

Application Owner: a company figure with extensive decision-making responsibilities on an application, usually the Process Owner or his/her delegate.

System Administrator (AdS): a professional person responsible for the technical management and maintenance of a processing system and its components. In the capacity of Machine Administrators of all Workstations, the System Administrator may come into contact with personal and/or confidential information.
The System Administrator has advanced access permissions to computer resources as he/she must be able to ensure continuous service and be able to carry out administrative or systems operator activities (e.g. administrators of networks, operating systems, databases, applications, access permissions, etc.) necessary for the management of an infrastructure supported by an application or service (system profile) or the management of the application (application profile). The professional figures to whom these administrative rights are granted are formally charged by the company in writing and are also reported to the internal Information Security Team.

Credentials: the identifying data of a user or an account (generally the UserID and Password).

Computer Data: any representation of facts, information or concepts in a form suitable for processing in a computer system,

including a program suitable for causing a computer system to perform a function.

Crimes related to the Infringement of Copyright: the crimes pursuant to Article 25-*nonies* of the Decree.

Computer Crimes: the crimes pursuant to Article 24-*bis* of the Decree.

Electronic Document(s): the electronic representation of acts, facts or legally relevant data.

Electronic Signature: the whole of the electronic data attached or connected by logical association to other electronic data, utilized as a method for digital authentication.

Copyright Law: Law No. 633 dated April 22, 1941 on Copyright.

Password: a sequence of alphanumeric or special characters necessary to authenticate to a computer system or application.

Peer to Peer: a mechanism for sharing digital content over a network of personal computers, normally used to share files containing audio, video, data and software.

Security Plan: a document which defines a set of coordinated activities to be undertaken to implement the security policy of the system.

Workstation: a computer terminal that can be fixed or mobile and that is capable of handling business information.

Information Security: the set of organizational, operational and technological measures aimed at protecting the information processing carried out through electronic means.

Information Systems: the network and the set of corporate systems, databases and applications.

Spamming: the act of sending numerous unsolicited messages, usually implemented using electronic mail.

Virus: a program created for the purpose of sabotage or vandalism, which may degrade the performance of computer resources, destroy stored data as well as spread via removable media or communication networks.

H.1 COMPUTER CRIMES AND ILLEGAL DATA PROCESSING (Article 24-*bis* of the Decree) AND INFRINGEMENT OF COPYRIGHT (Article 25-*nonies* of the Decree)

Below is a brief description of the crimes that are contained in this Special Section "H", pursuant to Article 24-*bis* and Article 25-*nonies* of the Decree. In this regard, it should be noted that although the two types of crimes protect different legal interests, it was decided to prepare a single Special Section for the following reasons:

- both cases require the proper use of computer resources;
- because of this, at-risk areas partly overlap;
- in both cases, the procedural rules are intended to raise the awareness of the Recipients about the multiple consequences of improper use of computer resources

H.1.1 TYPES OF COMPUTER CRIMES AND ILLEGAL DATA PROCESSING (Article 24-*bis* of the Decree)

- ***Electronic Document Forgery (Article 491-bis of the Italian Criminal Code)***

The rule provides that all crimes relating to the falsification of documents as provided for by the Italian Criminal Code (see Chapter III, Title VII, Book II), including ideological and material misrepresentation, both in official and private documents, are punishable even if such conduct does not involve a paper document but an official or private Electronic Document of evidential value (as an electronic representation of acts, facts or legally relevant data).

In particular, it should be noted that "material falsehood" occurs when a document is created or signed by a person other than the intended sender or signer, with some differences between the alleged author and the real author of the document (forgery) that is when the document is counterfeited (thus altered) through additions or deletions to the original document.
Ideological falsehood occurs, contrarily, when the document is not truthful, i.e. when it is not counterfeited or altered but contains untrue statements.
In the case of ideological falsehood, thus, it is the author of the

document who states untruthful facts.

Therefore, Electronic Documents are granted the same legal value as traditional paper documents to all intents and purposes.

By way of example, the crime of Electronic Document Forgery is committed when a person falsifies business records that are part of an electronic information flow or when a person alters information that is stored on his/her system and that has evidential value for the purpose of eliminating data that are deemed "sensitive" in view of a possible inspection.

- ***Unauthorized access to an information or telecommunication system (Article 615-ter of the Italian Criminal Code)***

This crime is committed when a person gains unauthorized access to an information or telecommunication system protected by security measures.

In this regard, it should be noted that legislators intended to punish the unauthorized access to an information or telecommunication system tout court, and thus even when, for example, such access does not cause proper data corruption: for example, a situation where a person, who has gained illegal access to a computer system, prints the contents of a document that was stored in the database of someone else's personal computer, while not removing any files, but merely copying information (unauthorized copy access), or simply displaying and reading information (unauthorized read-only access).

This type of crime is also committed when a person, while having gained authorized access to the system, remains in it against the will of its owner, and, according to prevailing case law, when the person has used the system to pursue a purpose other than the authorized one.

The crime could therefore theoretically occur in a situation where a person gains illegal access to a computer system owned by a third party (outsider hacking) to acquire someone else's confidential business information, or where a person gains illegal

access to corporate information to which he would not have legitimate access in view of the completion of further activities in the interest of the company.

- ***Unauthorized possession and distribution of computer or telecommunication systems' access codes (Article 615-quater of the Italian Criminal Code)***

This crime is committed when, in order to obtain a profit for himself/herself or for another or to cause damage to others, a person illegally gets hold of, reproduces, propagates, transmits or delivers codes, passwords or other means for the access to an information or telecommunication system protected by security measures, or otherwise provides information or instructions for the above purpose.

Article 615-*quater* of the Italian Criminal Code, therefore, punishes the acts committed by a person in connection with the illegal access in so far as they are aimed at getting hold for himself/herself or for another person of the means to circumvent the protective barriers of an information system.

The devices which can allow unauthorized access to an information system comprise, for example, codes, passwords or other means (such as badges or smart cards).

This type of crime is committed whether the person, who is in lawful possession of the above mentioned devices (for example a system operator), transmits them to a third party without authorization, or whether the person gets hold of one of these devices unlawfully.

Moreover, Article 615-*quater* of the Italian Criminal Code punishes whoever provides instructions or directions that are suitable for recreating the access code or circumventing the security measures of a system.
An employee of a company (A) may be guilty of this crime if he/she transmits to a third party (B) the Password to access the electronic mailbox of a coworker (C) with the purpose of allowing B to check on the activities carried out by C when this may result in a specific benefit or interest to the company.

- ***Distribution of electronic equipment, devices or computer programs aimed at damaging or interrupting a computer or telecommunication system's operation (Article 615-quinquies of the Italian Criminal Code)***

The crime is committed when a person, in order to illegally damage an information or telecommunication system and the information, data or programs contained therein, and cause the partial or total interruption or alteration of the system's operation, gets hold of, transmits, produces, reproduces, imports, disseminates, communicates, delivers or otherwise provides any third party with computer equipment, devices or programs.

This crime is committed, for example, when an employee, in order to destroy documents that are deemed "sensitive" with regard to ongoing criminal proceedings against the company, gets hold of a Virus suitable for damaging or interrupting the operation of that company's computer system.

- ***Wiretapping, blocking or illegally interrupting computer or information technology communications (Article 617-quater of the Italian Criminal Code)***

This crime is committed when a person fraudulently intercepts the transmissions of a computer or telecommunication system or between multiple systems, or prevents or interrupts such transmissions and when a person publicly discloses the partial or total contents of communications through any information means.

Interception techniques make it possible, during the transmission of data, to acquire the contents of communications between information systems or change their destination: the purpose of the illegal act is typically to violate the confidentiality of messages, compromise their integrity, delay them or prevent them from reaching their destination.

This crime is committed when, for example, in order to obtain an advantage for a company, an employee prevents specific communications from taking place through an information system so that a competing company is unable to transmit data relative to and/or an offer in a bid.

- ***Installation of devices aimed at intercepting, blocking or interrupting computer or information technologies communications (Article 617-quinquies of the Italian Criminal Code)***

This type of crime is committed when a person, except for the cases permitted by law, installs devices suitable for wiretapping, preventing or interrupting the transmissions of an information or telecommunication system, or between multiple systems.

The conduct prohibited by Article 617-*quinquies* of the Italian Criminal Code is therefore the mere act of installing this type of devices, regardless of whether or not they are used, provided they have the potential to cause damage.

The crime is committed, for example, to the advantage of the company, when an employee makes a fraudulent access to the office of a potentially competing commercial counterpart for the purpose of installing devices suitable for wiretapping the transmissions of computer and information technologies systems that are relevant to a future business negotiation.

- ***Damaging computer information, data and programs (Article 635-bis of the Italian Criminal Code)***

This crime is committed when a person destroys, deteriorates, deletes, alters or suppresses information, data or computer programs of others.

The damaging may be committed to the advantage of the company where, for example, the deletion or alteration of a file or a newly purchased computer program may be carried out to eliminate the proof of debt by a supplier of a company or to challenge the proper performance of obligations by the same supplier or in the event that "incriminating" corporate data is damaged.

- ***Damaging electronic information, data and programs used by the Government or any other public organization or public service (Article 635-ter of the Italian Criminal Code)***

This crime occurs when a person commits an act intended to destroy, deteriorate, cancel, delete, alter, or suppress computer information, data or programs used by the Government or any other public organization, or pertaining to them, or otherwise of public service.
This crime differs from the previous one since in this case the damage is perpetrated against the property of the Government or other public organization or public service; it follows that the crime occurs even when data, information or programs are privately owned but are intended to satisfy the public interest.
This crime could be committed in the interest of a company, when, for example, an employee destroys electronic documents of evidential value regarding ongoing criminal proceedings against that same company that are filed with public authorities (such as the police).

- ***Damaging computer or telecommunication systems (Article 635-quater of the Italian Criminal Code)***

This crime occurs when a person, by committing the crimes pursuant to Article 635-*bis* of the Italian Criminal Code, or by introducing or transmitting data, information or programs, destroys, damages, renders useless, totally or partially, computer or telecommunication systems of others or severely hinders their normal operation.

Therefore, the crime of damaging computer systems and not the crime of damaging data pursuant to Article 635-*bis* of the Italian Criminal Code is committed when the alteration of data,

information or programs renders useless or severely hinders the normal operation of a system.

- ***Damaging computer or telecommunication systems of public service (Article 635-quinquies of the Italian Criminal Code)***

This crime is committed when the conduct pursuant to the above mentioned art 635-quater of the Italian Criminal Code is intended to destroy, damage, render useless, totally or partially, computer or telecommunication systems of public service or to severely hinder their operation.
With regard to the crime of damaging computer or telecommunication systems of public service, unlike the crime of damaging data, information and programs of public service pursuant to Article 635-ter of the Italian Criminal Code, the relevant circumstances are that firstly the whole system is damaged and secondly that the system is for public service, regardless of whether the system is privately or publicly owned.

- ***Computer crime by the certifier of a digital signature (Article 640-quinquies of the Italian Criminal Code)***

This crime is committed when a person providing Digital Signature certifying services, in order to obtain for himself/herself or others an undue profit or to cause damage to others, infringes the obligations provided by law relating to the issuance of qualified certificates.

This crime is therefore a so-called proper crime because it can only be committed by a person who can issue qualified certificates, or rather, by certifiers of qualified Digital Signatures.

*****

It should be noted, however, that the occurrence of any of the above mentioned computer crimes is relevant, for the purposes of the Decree, only in the event that the conduct, regardless of the nature of the data, information, programs, computer or telecommunication systems -whether they are corporate or not- is to the advantage of TERNA PLUS.

Therefore, in the description of the single crimes, as well as in the following description of the Crimes relating to the Infringement of Copyright, such relevant aspect was taken into account for the preparation of the proposed case studies.

With reference to the commission of Computer Crimes, a pecuniary sanction ranging between 100 and 500 shares (considering that the value of each share is determined on the basis of the financial and property situation of the Corporation, between a minimum of € 258 and a maximum of € 1549 and that they can range between a minimum of approximately € 26,000 and a maximum of € 800,000) and a disqualifying measure may be imposed on the Corporation depending on the type of crime committed.

H.1.2 TYPES OF COMPUTER CRIMES AND INFRINGEMENT OF COPYRIGHT (Article 25-*nonies* of the Decree)

Article 25-*nonies* provides for a number of crimes pursuant to the Copyright Law (and, in particular, to Articles 171, 171-*bis*, 171-*ter*, 171-*septies* and 171-*octies*) such as, for example, the import, distribution, sale or possession for commercial or business purposes of programs contained on a medium not bearing the SIAE stamp; the reproduction or reuse of database contents; the illegal duplication, reproduction, transmission or public dissemination of intellectual works for television or cinema; the introduction of an intellectual work protected, in part or totally, by copyright, into a telecommunication network system through any type of connection.

A preliminary analysis showed the immediate inapplicability to TERNA PLUS and to the other Group Companies of cases under

articles 171-*ter*, 171-*septies* and 171-*octies* of the Copyright Law.

The following is therefore a brief description of the two types of crimes under art 25-*nonies* of the Decree that are considered *prima facie* relevant to the Company, provided for by articles 171 paragraph 1, subparagraph a *bis* and paragraph 3, and Article 171-*bis* of the Copyright Law.

- **Crimes connected to copyright protection and other rights connected to its exercise (Article 171 paragraph 1, subparagraph a *bis* and paragraph 3 of the Copyright Law)**

In relation to the crimes pursuant to Article 171, the Decree exclusively takes into consideration two instances, namely:

(i) the act of making available to the public, by introducing into a telecommunication network system, through connections of all kinds, an intellectual work that is partially or totally protected; (ii) the act of making available to the public, by introducing into a telecommunication network system and through connections of all kinds, an intellectual work not intended to be used for advertisement, or through the usurpation of authorship, or the distortion, mutilation, or other modification of the work itself that would be prejudicial to the honor or reputation of the author.

In the first case, it is the author's financial interest in the work that is protected; the author's earning expectation would in fact be compromised in the event that his/her work is freely distributed over the network; and, in the second case, the protected legal right is clearly not the author's earning expectation but his/her honor and reputation.

Such a crime could be committed in TERNA PLUS' interest or in the interest of another Group company if, for example, the content of a work protected by copyright is loaded into TERNA PLUS' website or into the website of another Group Company.

- **Copyright protection and other rights connected to its exercise (Article 171 *bis* of the Copyright Law)**

Said provision is designed to protect the proper use of software and databases.

With regard to software, a crime is committed in the case of unlawful duplication or import, distribution, sale and possession for commercial or business purposes and rental of "pirated" programs.

This crime is committed when, in order to obtain a profit, a person unlawfully duplicates computer programs, or for the same purpose, imports, distributes, sells or holds for commercial or business purposes or rents programs contained on media not bearing the SIAE stamp.

The act is punished even when the conduct relates to any means where the sole intended purpose is to enable or facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

The second paragraph punishes anyone who, in order to obtain a profit, reproduces on media not bearing the SIAE stamp, transfers onto another medium, distributes, communicates, presents or shows to the public the contents of a database or extracts or reuses a database or distributes, sells or rents a database.

At the subjective level, the crime is committed even when there is a will to achieve a benefit, therefore also when there are acts that are not prompted by the specific purpose of obtaining a purely economic gain (such as the assumption of obtaining an advantage).

Such crime could be committed in the interest of the company when, for example, in order to save the cost associated with licensing for the use of an original software, non-original programs are used for business purposes.

*****

With reference to the commission of the Crime of Copyright Infringement, a pecuniary sanction of up to 500 shares (therefore up to approximately €800,000) and a disqualifying penalty may be imposed on the Corporation, such as the

prohibition of exercising activities or the suspension or revocation of authorizations, licenses or permits that may be used to commit the offense, for a period not to exceed one year.

H.2 AT-RISK AREAS

With regard to the crimes and criminal conduct set out above, the areas deemed more specifically at risk are:

a. With specific reference to computer crimes:

1. management of corporate Information Systems to ensure their operation and maintenance, the evolution of the technological and applicative IT platform as well as Information Security;

2. management of electronic information flow with the public administration;

3. provision of IT services and any other external resource whose contract includes the use of a computer license and/or a computer service (for example, cloud services including software as a service - Saas) and/or requires interaction with a company computer system by departments that do not have full responsibility for IT matters;

b. With specific reference to crimes in infringement of copyright:

1. management of content on websites relative to TERNA PLUS and social media profiles, as well as the management and organization of events.

All At-Risk Areas as indicated above take on importance - as a caution - also if the activities that form their objective are carried out by the Parent Companies or by another Group Company – fully or partly – in the name of and/or on behalf of the Company, by virtue of the agreements signed or of specific proxies granted.

For the activities carried out in the name of and/or on behalf of the Parent Company, the Companies shall implement the reporting activity according to the terms indicated in the General Section and in the individual Special Sections.

The Companies shall inform the Parent Company of any criticalities deriving from the application of the strategic guidelines that contrast with the model adopted.

TERNA PLUS' CEO may add other At-Risk Areas to the ones described above, identifying the relevant profiles and defining the most appropriate actions.

H.3 RECIPIENTS OF THIS SPECIAL SECTION: GENERAL CONDUCT AND IMPLEMENTATION RULES

The Objective of this Special Section is that the Recipients - to the extent to which they may be involved in operating in At-Risk Areas and considering that each of these persons has a different position and various obligations towards TERNA PLUS and the other Group Companies – should comply abide by rules of conduct that comply with those established in the document, in order to prevent and avoid the occurrence of Computer Crimes and those of Infringement of Copyright.

In particular, the function of this Special Section is to:

a) provide a list of the general rules as well as the specific procedural rules which the Recipients must comply with for the correct application of the Model;

b) provide the Vigilance Body, as well as the directors of company departments called to cooperate with the Body, the operational principles and tools for carrying out the necessary checks, monitoring and verifications entrusted to them.

In carrying out all activities regarding the management of the company, in addition to the rules in this Model, Company Representatives – with respect to their activity - will generally be expected to be familiar with, and comply with, all the procedural rules adopted by the Parent Company and transposed by the Company as well as any procedures provided for by TERNA PLUS contained, for example, in the following documents:

1. the Code of Ethics;
2. the company organization chart and patterns;
3. Guideline LG018 on the Information Security Policy - Strategic Policies and their relative applications:

- IS Glossary (R00LG018)
- Acceptable use of computer resources (R01LG018)
- Launch of the Information Security Framework (R02LG018)
- Creation and maintenance of the Security Posture of the Information Security Framework (R03LG018)
- Logical access control of computer resources (R04LG018)

- Network and communications security (R05LG018)
- Physical and environmental security of computer systems (R06LG018)
- The security of information in the employees' life-cycle and in relations with third parties (R07LG018)
- Security of IT assets (R08LG018)
- Security Incident Management (R09LG018)

4. Operational instructions regarding the methods of Cataloging Types of Information (IO510SA);
5. Definition of Information Security Assessment activities (IO515SA);
6. Internal memorandum that maps the roles and company representatives assigned Responsibilities and duties in the Group for Information Security (NI067SA);
7. Regulation on the roles, responsibilities and principles of the Chief Risk Officer of the TERNA Group (LG044);
8. Guideline that regulates the methods and authorization procedure to be followed for the provision of IT services (LG027);
9. Operational instructions that describe the methods of purchasing professional IT services through the use of the Framework Agreements and Closed Contracts, aimed at developing software applications, progressive maintenance and performance (IO110RE);
10. Guideline that defines the criteria for the assignment and management of IT and company communication resources (LG015);
11. Operational instructions that describe the management (creation, modification, periodic review and override) of access credentials for services, applications, databases and operating systems (IO317SI);
12. Operational instructions regarding License Management (IO309SI);
13. Operational instructions on the management of

Backup and Restore procedures and removable devices (IO326SI);

14. Internal memorandum that identifies ICT Management Representatives (NI-ICT);
15. Manual on the management of Incident, Change, and Problem Solving in requests for activities and maintenance at workstations and the management of related infrastructure (IO311PM);
16. Operating instructions on "Access Control – access modes for corporate offices" (IO410SA);
17. Operating instructions that define the management obligations of System Administrators (IO513SA);
18. Operating instructions on Internet browsing and email security (IO414SA);
19. Guideline on the use of Social Media by Terna Group Personnel (LG045);
20. Guideline on the appointment of consultancy roles and duties for the provision of professional services to third parties (LG025);
21. Guideline on entrustment to the appointed economic operator (LG030).

H.4 SPECIFIC PROCEDURAL RULES

In order to ensure adequate compliance within each At-Risk Area, the following rules are laid down which must be respected by TERNA PLUS, Company Representatives and other subjects who may be authorized to access these areas, it being understood that the implementation rules are included in the corporate policy and procedures as well as in the organizational documents which are referred to, by way of example, in the previous paragraph H.3.

In particular, the following activities are prohibited:

1) connect to the Group's information systems, personal computers, peripherals and other equipment or install any software without prior permission of the designated company subject in charge;
2) install any software product in violation of the license agreements and, in general, in violation of all copyright laws and regulations;
3) change the software and/or hardware configuration of fixed or mobile workstations with the exception of cases provided for by a corporate rule or upon proper authorization;
4) purchase, hold or use software and/or hardware tools - except for duly authorized cases where such software and/or hardware is used to monitor the company's information systems for security purposes - which could be used improperly to evaluate or compromise the security of computer or telecommunication systems (systems to detect Credentials, identify vulnerabilities, decrypt encrypted files, wiretap traffic, etc.);
5) obtain Credentials to access company information and telecommunication systems as well as those of customers or any third party, according to methods or procedures other than those authorized for such purposes by TERNA PLUS;
6) disclose, sell or share one's own Credentials with TERNA PLUS' employees or external staff and with the employees of external staff of other Group Companies to access the company network and systems or those of customers or any third party;

7) illegally access the information system of others - that is used by other Employees or any third party - or access it to tamper with or alter any data contained therein;

8) tamper with, remove or destroy company information or that of customers or any third party, including archives, data and programs;

9) exploit any vulnerabilities or inadequacies in the security measures of company computer or telecommunication systems or those of any third party, to gain access to information and resources other than the ones which one is authorized to access, even if such intrusions do not cause damage to data, programs or systems;

10) acquire and/or use products that are protected by copyright in violation of contract guarantees provided for the intellectual property rights of others;

11) illegally access the Company's website in order to illegally tamper with or alter any data contained therein or enter multimedia data or content (images, infographics, videos, etc.) in violation of copyright laws and applicable company procedures;

12) share with unauthorized TERNA PLUS' employees or external staff, information regarding the controls implemented on the company information systems and how they are used;

13) hide, render anonymous, or substitute one's own identity and send e-mails reporting false information or intentionally send e-mails containing Viruses or other programs that can damage or wiretap data;

14) Spamming as well as any action in response to it;

15) send through a company computer system any altered or forged information or data.

TERNA PLUS, in turn, shall undertake the following tasks:

1) adequately inform Employees and *interns* and other individuals – such as External Contractors – who may be authorized to use the Information Systems of the importance of the following:

- ensure the confidentiality of their Credentials and not disclose the same to third parties;

- properly use software and databases;

- not enter data, images or other material protected by copyright without the prior permission of one's supervisors according to the instructions contained in the company policy;

2) provide recurrent training for Employees in compliance with their duties and, to a lesser extent, for *interns* and other individuals - such as External Contractors – who may be authorized to use the Information Systems, in order to raise their awareness of the risks posed by the improper use of corporate computer resources;

3) define what is considered acceptable conduct for the proper use of software and databases in the Code of Ethics and Information Security policy;

4) have Employees as well as *interns* and other individuals – such as External Contractors – who may be authorized to use the Information Systems, sign a specific document in which they commit to the proper use and protection of corporate computer resources;

5) inform Employees as well as *interns* and other individuals – such as External Contractors – who may be authorized to use the Information Systems, of the need to never leave their systems unattended and to lock them using their access codes, should they leave their Workstation;

6) set up their Workstations in a way that after a given period of time of inactivity, the computers will automatically lock;

7) protect, as far as possible, every corporate computer system to prevent the illegal installation of hardware that can wiretap, prevent or halt communications relating to an information or telecommunication system, or between multiple systems;

8) provide information systems with the appropriate anti-virus and firewall software to ensure that, where possible, they cannot be disabled;

9) prevent the installation and use of software that is not approved by the group and that is unrelated to the professional activities carried out for the company;

10) inform users of computer systems that the software they use to carry out their activities is protected by copyright and as such it is forbidden to duplicate, distribute, sell or hold it for commercial and/or business purposes;

11) limit access to particularly sensitive Internet sites and areas as they can distribute and disseminate Viruses that can damage or destroy information systems or data contained therein and, in any case, implement - in the presence of union agreements – devices that are responsible for detecting possible abnormal Internet access sessions, by identifying the "index anomaly" and exchanging information with the appropriate departments in the event that such anomalies are detected;

12) prevent the installation and use on TERNA PLUS' information systems of Peer to Peer software through which it is possible to share any type of files (such as videos, documents, songs, Viruses, etc.) on the Internet network, without any control by TERNA PLUS;

13) if wireless connections are used for the connection to the Internet, protect them by establishing an access key to prevent any third party outside of TERNA PLUS from illegally logging onto the Internet through its routers and carrying out any illegal activities for which the Employees may be blamed;

14) provide an authentication procedure through the use of Credentials matching a limited profile of the system resource management, specific for each Employee, *intern* and other persons – such as External Contractors – who may be authorized to use the Information Systems;

15) limit access to the company computer system from the outside, by adopting and maintaining different authentication systems or others in addition to the ones that are in place for the internal access of Employees, *interns* and other persons – such as External Contractors – who may be authorized to use Information Systems;

16) immediately cancel the accounts of system administrators at the end of their contract relationship;

17) provide, in the contract relationship with Suppliers of software services and databases developed in connection with specific business needs, indemnity clauses designed to hold TERNA PLUS free and unharmed against any liabilities in case of acts that are committed by the Suppliers themselves and that may violate any intellectual property right of a third party. Include in these contracts, the signing of specific documents that bind them to the correct use and protection of corporate information resources which they may use.

With specific reference to the At-Risk areas referred to in Chapter H.2, section 4), the Company has regulated purchasing requests of external resources whose contract includes the use of IT services (such as cloud services including "software as a service - SaaS") by departments that do not have full responsibility for IT matters. In particular, LG025 and LG030 provide for the inclusion of a "flag" that the applicant must check if the requested service provides for an interaction or incorporates an IT service with the consequent sending of an authorization request to the ICT and Company Protection Departments. This provision ensures departmental segregation and a correct authorization and purchasing procedure for external resources.

H.5 INSTRUCTIONS AND INSPECTIONS OF THE VIGILANCE BODY

The VB's duties in relation to compliance with the Model regarding the crimes pursuant to Article 24 -*bis* and 25-*nonies* of the Decree are as follows:

- carry out periodic controls on compliance with this Special Section, and periodically verify the effectiveness of such controls in preventing the commission of the crimes provided for in Article 24 *bis* and 25-*nonies* of the Decree. In order to fulfill these obligations, the Vigilance Body, making use, if necessary, of the collaboration of expert advisors competent in these matters, will conduct periodic analyses of the system of prevention adopted in this Special Section and will suggest any action necessary to make improvements or changes to the competent offices of TERNA PLUS if significant violations of rules related to Cyber Crimes and/or Crimes of Infringement

of Copyright come to light, or when there are transformations in corporate organization and activities as a result of scientific and technological advances;

- propose standardized instructions, or collaborate in their preparation, with regard to the rules of conduct to respect in At-Risk Areas as defined in this Special Section. These instructions should be in writing and saved on hard copy and on computer file;

- examining any reports of alleged violations of the Model and carrying out any investigation deemed necessary or appropriate on the basis of the information received.

TERNA PLUS guarantees the implementation of data stream procedures between the VB and the directors of the relevant Departments, the 231 Representatives or other Company Representatives who may in any case be contacted by the VB whenever it deems appropriate.

The information to the VB shall be given timely should violations to specific procedural rules be detected as indicated in Chapter H.4 of this Special Section, or procedures, policies and company regulations regarding the above-mentioned At-Risk Areas.

The VB is also assigned the power to access, or request its delegates to access, all the documentation and all company's relevant sites for carrying out its duties.