INTEGRA LIFESCIENCES ITALY S.R.L.

Model of Organization, Management and Control

(pursuant Italian Legislative Decree 231/2001)

[TRANSLATED FROM THE ORIGINAL ITALIAN VERSION]

Special Part J

Information Systems Management

1. Special Part Aim

This Special Part aims to define do's-and-don'ts as well as control activities that all Addressees are required to adhere to and execute whenever operating within activities and process listed in subsequent chapter 2, for the purpose of *i)* preventing the risk of specific "231" relevant crimes commission as well as of *ii)* assuring correctness and transparency in conducting business activities.

In addition, this Special Part aims to provide Supervisory Body and all other control bodies with relevant information to perform their control activities.

Addressees should adhere to each of the extent applicable:

- Model of Organization, Management and Control, General Part;
- Standard of Business Conduct and Ethics;
- Delegation of Authorities in place;
- each and all other Company and Group documents addressing activities relevant for the Italian Legislative Decree 231/2001 compliance.

In general, all actions and behaviors in violation of existing and valid laws are forbidden.

2. Special Part Scope

This Special Part and, specifically, do's-and-don'ts as well as control activities detailed in the subsequent chapters, apply to all Integra managers, employees and other professionals involved with the "Information Systems Management" process.

3. Applicable 231 crimes

231 crimes theoretically applicable to Integra Lifesciences Italy S.r.l. are the following:

- Information Technology crimes and unlawful data processing (art. 24-bis Leg. D. 231/2001);
- violation of copyright and other related rights (art. 25-novies Leg. D. 231/2001);
- tax crimes (art. 25-quinquiesdecies Leg. D. 231/2001).

4. Do's-and-don'ts

All Addressees must:

- rigorously comply with the organizational procedures related to asset management and, in particular, to Integra's computer network, making appropriate use of it according to their work-tasks;
- avoid any behavior that may jeopardize security, privacy and integrity of organizational and third parties' information;
- avoid any behavior aimed at overcoming or bypassing the Company or other's (may them be public or private subjects) IT System protection;

- abide to the univocal and individual use of user-id to access the network applications;
- abide to a correct password management in compliance with the guidelines, shared with all users for the selection and utilization of the keyword;
- periodically verify the users' access, in any way, to data, systems and network;
- guarantee, with the use of applications, the traceability of data modifications made by users;
- define criteria and methodologies to assign, modify and delete user profiles;
- periodically analyze user profiles in order to verify that they are consistent with the assigned responsibilities;
- define the security measures adopted, the surveillance methods and related frequency, the responsibilities, the reporting process of violation / break-ins of the technical rooms or the security measures and countermeasures to be activated;
- file the documentation relative to every single activity in order to guarantee its absolute traceability.

It is explicitly forbidden to:

- illegally access (without prior authorization) a protected IT system;
- change, by using others' electronic signatures or in any way, computer documents as well as data and information contained in computer programs;
- destroy, deteriorate, erase, change, suppress information, data or computer programs of others, or even endanger the integrity and availability of information, data or programs used by the State or by other public body or relevant to them or in any case of public utility;
- produce and transmit documents in electronic format with false and/or altered data;
- obtain, duplicate, disclose, communicate or divulge access codes of protected or encrypted IT systems;
- install equipment aimed at intercepting third parties and obtain information that can be of the Company's interest or to its advantage;
- install equipment aimed at damaging hardware in the interest or to the advantage of the Company (e.g. access to backup copies and destruction of information that could qualify as proof of illicit actions);
- disseminate programs able to infect a system and sabotage the regular functioning (e.g. the IT system of a competitor);
- illegally use a copyright protected software without purchasing, all or partially, the necessary licenses;
- illegally duplicate programs covered by license in order to take advantage in terms of cost savings;
- include, in the Company website, creative work - or parts of it - protected by intellectual property rights, for which the Company has not obtained a legitimate license. For instance, scientific publications regarding drugs or derivatives marketed by the subsidiaries of the Group;

- conceal or destroy the accounting records or other similar documents saved and stored on the information systems used by the Company, in order not to make the income or volume of business rebuildable.

5. Information Systems Management

The activities related to the Information Systems Management (i.e.: Global Technology / Information System) are managed by the Corporate Information Technology Function (ILS-Corp US) under a special service contract, to be refer to.

Here follow the control activities to be put in place, within Information Systems Management.

Management of logical access to data and systems

- Each employee is provided with a logical access and a PC connected to the Company's network;
- access to organizational tools is allowed only to authorized personnel, through an univocal identification of the user;
- access to organizational tools, as well as shared folders, is based on the job position;
- with specific reference to the organizational information systems, access clearance, as well as every deletion or modification of a user, may be required by the Identity Manager only;
- the user identification occurs with username and password. Every new employee is provided with a temporary password to be modified at the first log-in;
- the communication of passwords to access organizational tools takes place confidentially and each employee is responsible for its safeguard and non-disclosure;
- systems automatically require a password update every 90 days;
- periodical monitoring activities of access to organizational tools and reviews of active users are conducted in order to guarantee an accurate profiling and privileges clearance on the system;
- each employee is provided with an individual e-mail account to be used exclusively for work purposes.

Back-up management

- The Company shall have periodic backup plans of data, files, programs and operating systems, in order to guarantee the safeguard of the Company's information property;
- data backup is performed through removable storage units;
- restore tests are performed periodically.

Management of software, equipment, device or IT programs

- The workstations shall be equipped exclusively with software with legitimate license;
- it is forbidden to download software of any kind at the workstations.

Management of network security

- Server and client shall be equipped with antivirus software automatically updated;

- the e-mail server shall be equipped of anti-spam, anti-phishing and antivirus filters;
- internet access shall be filtered through an automatic web filtering system.

Physical security management

- The Corporate IT Function is in charge for the management of CED room;
- access to the CED room is allowed to authorized personnel only and it is monitored with an entry log.