CORPORATE SECURITY GUIDELINES

I. Purpose of the Policy

BSP Pharmaceuticals Spa ("BSP") is committed to protecting its people, information and assets; complying with legal and regulatory requirements and meeting industry standards and best practices.

These guidelines are designed to mitigate threats of intentional harm against Personnel, facilities, physical infrastructure and physical property and to ensure compliance with BSP's security regulations and the applicable standard operating procedures.

II. Application

These guidelines applies to all officers, employees, customers and suppliers (collectively, "Personnel").

III. Features

a. Personnel
b. Physical Security
c. Facility Security Measures
d. IT Security
e. Related Policies

- **PERSONNEL**

All Personnel shall comply with this Policy, rules and standards made pursuant to it.
The Personnel shall refrain from carrying out any action that may be in conflict with the interests of BSP and adopt a dutiful and loyal behavior also towards BSP to meet the obligations set out in the employment contract, this, the Code of Conduct, BSP's standard operating procedures, the Organisational, Management and Control Model in accordance with Italian Legislative Decree 231/2001, the Business Continuity Plan, the Supplier Code of Conduct and BSP's values.
All reasonable steps shall be taken by Personnel to protect BSP assets in its possession or under its control by demonstrating security awareness in the execution of any of its duties.

- **PHYSICAL SECURITY**

It is BSP's policy to provide Personnel with a safe workplace. Monitoring those who enter and exit the premises is a good security practice for identifying the authorized persons on BSP's premises and minimizing risk to BSP's systems and data. BSP has established the following guidelines for the use of magnetic identification badge:

a. Employees, officers and directors are equipped with magnetic identification badge.
b. Non-employees/visitors are equipped with generic visitor badge. Visitors should be given only the level of access to BSP's premises that is appropriate to the reasons for their visit. After checking in, visitors shall be escorted in BSP's premises.

The badge is strictly personal and employees and non-employees shall wear it in a visible manner within BSP's campus. The employee/non–employee shall reach out to the Personnel Administration Office in order to report any loss/theft or malfunction of personal identification badge. It will be the responsibility of the Personnel Administration Office to ensure the issuance of a new personal identification badge through the Information Technology system.
Access to the workplace is possible only during the working hours. If the Personnel needs to access to BSP's campus out of working hours, the Personnel shall be authorized by the relevant manager and/or BSP's key contact in case of visitors.

- **FACILITY SECURITY MEASURES**

It is BSP's policy to ensure the security of its own property and fences through the following Facility Security measures:

a. Video surveillance active 24/7/365
b. Perimeter alarm
c. Guard gate manned 24/7/365
d. Nightly armed surveillance service
e. Segregated Employee parking area from the loading and/or shipping areas
f. Lighting system ensuring nightly illumination of the entire facility

- **IT NETWORK SECURITY POLICY**

BSP has adopted specific measures to protect the security of its IT system and structure to ensure that users connecting to the corporate network are authenticated in an appropriate manner and in compliance with BSP's standard procedures.

Website: The Personnel shall be responsible for internet browsing, accessing to websites, downloading of images, audio or music files and/or video files. Internet browsing for personal purposes (such as: social networks and/or instant messaging systems, blogs, discussion forums) is not allowed, as well as, Internet connection sharing and connection to external VPN Server.

Authentication: For the use of the personal account and the access to the machines and BSP network the user shall:

a. be authenticated against the domain at setup. If the domain is not available or the authentication cannot occur for any reason, the access to machines and network is not permitted;
b. keep the personal passwords confidential and exclusive;
c. keep the account personal only. Accounts sharing and group accounts are not permitted.
d. pay the utmost attention to files of external origin by warning immediately the personnel of IT Department in the event that viruses are detected.

IV. RELATED POLICIES

a) Code of Conduct
b) BSP's standard operating procedures
c) Organisational, Management and Control Model in accordance with Italian Legislative Decree 231/2001
d) Business Continuity Plan
e) Supplier Code of Conduct