Information Security Policy

The various new threats newly derived from global security requirements and technology development may cause serious impact on the information system and its assets of GC Biopharma. Corp. (hereinafter referred to as the "company"). The information security activities shall become an indispensable factor for secure company. Therefore, all executives and employees should do their best to preserve the information assets of company based on information security policy as below.

First, executives and employees must recognize and handle the information as an important asset to be protected. Go through the user identification and authentication procedures when access to major information assets. Also, do not leak or disclose any information to outsider without the approval from the head of department.

Second, executives and employees must receive the information security education at appropriate level corresponding to their job duties in order to recognize the importance of information security and develop its capabilities. In addition, the information security activities should be motivated by establishing and implementing fair reward and punishment standards.

Third, all policies and guidelines related to information security must be established to ensure confidentiality, integrity, and availability of assets, and these activities must be consistently promoted by the information security department.

Fourth, the company's assets must be classified according to their value and importance, and managed based on official procedures under their grade. The value of assets should be regularly re-evaluated and reflected in information security policies and guidelines.

Fifth, the information assets must be accessed only by authorized personnel as appropriate standards, and the areas where important information assets are operated and managed must be protected from various disasters and accidents such as access by unauthorized persons, power outages, fire, and flood damage.

Sixth, even if the information assets are damaged by intrusion and intentional or accidental intrusions by internal/external persons, the company must be able to continue in business, and the intrusion response plan should be established and managed to minimize damage by quickly recovering information assets.

Seventh, the information system operation in company must be appropriately distributed considering the

job characteristics and performed according to predefined procedures. By maintaining and managing the information system operation records, the records should be reflected in the establishment of information system operation plans for future and in the event of an intrusion accident.

Eighth, any measures must be taken to secure the information system from harmful software and do not leak the information assets to outside or deteriorate the system performance caused by use of information system not related to work.

Ninth, all information security activities must comply with the relevant guidelines of the holding company and laws related to intellectual property rights and personal information security. In addition, it should be periodically confirmed that security activities shall be accurately carried out according to guidelines and procedures.

All executives and employees must do their best to secure information system, recognizing that successful information security activities of GC Biopharma Corp, which has a half-century history, are a shortcut to global corporate competitiveness.