Information Security Declaration

As a global leader in the health industry for the human future, information system and information related to provide internal & external service shall be the major assets of GC Biopharma. Corp. (hereinafter referred to as the "company") and performing duties in efficient shall be hard without providing reliable internal and external service. Therefore, the management in company has an obligation to secure and improve the information system and its information, this means that appropriate measures must be taken to protect information system from various threats such as errors, destruction, terrorism, personal information leakage, service interruption and natural disasters.

The company should confirm and prepare for various security problems expected when operating and managing the information system in the future. This is because system problems expected under operation and management process such as hacking, illegal leakage and access, rapid and widespread malicious computer virus infection and other issues. Hence, in thoroughly consideration of delay or degradation in work performance and various legal, social and ethical issues caused by major information loss or information incident, the appropriate preparation according to these problems shall be highly necessary day by day.

Therefore, company information must be secured based on its values and the security measures should be applied to all media where information is stored, system process and transmission. These measures include limited access only for essential business performance. The company managers should support sufficient time and resources to adequately protect information system and supplementary measures should be devised and implemented to minimize information exposure when they are confirmed as deficient preparation for information security.

To achieve thorough information security system in company, the participation and cooperation with all employees in company are required and enough education reference to support this should be provided. All information security activities including the introduce and revision of its polices, guidelines and procedures required to operate the information security system, should be conducted by officially designated chief information security officer and related department. Also, all employees should follow their control. Finally, independent security audits should be regularly performed in order to confirm that the information security system is thoroughly established and operated.

Eun-chul Huh, CEO of GC Biopharma