Information Security Policy

Article 1 (Purpose)

This Policy provides for the basic requirements for protecting and effectively using information assets and carrying out prescribed business processes in the course of business activities promoted by Santen Pharmaceutical Co, Ltd. (“Santen Japan”) and its group companies (individually, a “group company,” which includes Santen Japan, and collectively, the “Santen Group”) in accordance with the Santen Group’s mission statement and the Information Security Policy Statement established based thereon, for the purpose of gaining social trust in the Santen Group and enhancing its business activities.

Article 2 (Positioning of This Policy)

This Policy describes the basic concepts and direction for security of the Santen Group’s information assets and provides for the guiding principles to be followed in the Santen Group. This Policy has been established to specify the information security management scheme, responsibilities and authorities, and basic requirements for the Santen Group’s information security management, which constitute the framework for putting the philosophy in the Information Security Policy Statement into action. All Information Users, including officers or supervisors responsible for controlling respective information assets, are required to properly perform their duties for ensuring security of information assets in accordance with this Policy.

Article 3 (Scope of Application)

This Policy applies to all information assets associated with the Santen Group’s business activities and is binding upon all Information Users and all organizational units, offices and entities in the Santen Group.

Article 4 (Structure)

An Information Security Administration Team shall be set up for making policies for supervisory activities for the Santen Group’s information security and making decisions on other related issues. Information Systems Supervisors shall check the risks associated with the information assets falling within the scope of their own responsibility and verify the effectiveness of the measures against such risks, based on the findings from inspections of the information assets and reviews conducted in

accordance with the Information Security Detailed Rules etc, and shall implement necessary measures for improvement to ensure specified security levels for respective information systems.

Article 5 (Proper Control of Information)

To protect the Santen Group's information from threats to security (intentional threats, among others) and facilitate effective use of the Santen Group's information, Information Supervisors shall identify the pieces of information falling within the scope of their own responsibility and maintain appropriate management in accordance with the evaluation level.

Article 6 (Incident Response)

To track and record event logs in information systems, which will serve as evidence of activities in the information systems, Information Systems Supervisors and Information Systems Administrators shall carry out the steps specified in the Information Security Detailed Rules etc. In the event of an incident, information shall be promptly shared with relevant departments, and an appropriate organizational framework shall be established to ensure an effective response.

Article 7 (Education and Training)

The Information Security Administration Team shall, with the cooperation of Information Supervisors, formulate and implement education and training programs for Information Users with the aim of raising their awareness about the importance and necessity of information security and ensuring their compliance with this Policy and their proper management and operation of information assets.

The Information Security Administration Team shall, considering the effectiveness of education and training and the latest trends in the threats to security, develop and improve programs conducive to improving Information Users' security awareness more effectively. To make sure that each employee in service or each business partner under contract with a group company recognizes and fulfills their responsibilities pertaining to information security, the relevant Information Systems Supervisor and Information Supervisor shall carry out the steps specified in the Information Security Detailed Rules etc.

Article 8 (Outsourcing Management)

If any operation involving the handling of the Santen Group's information assets is

outsourced, or if any information asset is shared with a third party, or if any cloud service operated by a third party is used for handling information assets, the manager responsible for arrangement of a relevant agreement with the third party concerned shall clarify the security measures to be incorporated in the agreement and specify the procedures for reporting, roles and responsibilities upon occurrence of a security incident.

Article 9 (Assessment of Risks and Examination of Countermeasures)

Santen group shall instruct Information Systems Administrators to regularly assess risks associated with each information asset in terms of confidentiality, integrity and availability, and record the results of the assessment based on the assessment results and acceptable risk levels derived therefrom, Information Systems Supervisors (or the relevant Information Supervisor) shall consider countermeasures.