Daiichi Sankyo Group
Information Security Policy

Daiichi Sankyo Co., Ltd.

Daiichi Sankyo Group recognizes proper management of information as a key management issue, and defines the basic policy on information security as "Information Security Policy ".

Establish a Chief Information Security Officer (CISO)

Daiichi Sankyo Group (hereafter referred to as DSG) shall establish a Chief Information Security Officer (CISO), who is responsible for enacting information security policy, and maintain information security measures for all DSG operating companies globally under the CISO's leadership.

Build an information security management system

In order to protect the information assets of the organization and to control them appropriately, DSG shall build an organization for prompt action on information security measures with the appointment of information security managers for each global affiliate under the supervision of the CISO.

Establish internal rules for information security

DSG shall establish internal rules of information security and ensure that every employees follows the guidelines and rules for protecting and managing information assets properly.

Comply with laws and regulations

DSG shall comply with laws and regulations related to information assets as well as contractual requirements and obligations related to information security.

Implement essential information security measures

DSG shall implement the organizational, human, physical and technical safeguards in order to prevent information security violations of intellectual property, including unauthorized access, leakage, falsifications, and corruption.

Improve information security awareness

DSG shall regularly educate and train every employee, temp workers, consultants etc (every user of information assets of the organization) to improve information security awareness and proper use of information assets.

Correspond with business partners

DSG shall audit information security practices at business partners and ensure that they maintain appropriate information security levels.

DSG shall improve information security in the organization's entire supply chain through cooperation with business partners.

Deal with confidential information supplied by business partners

DSG shall properly protect and manage confidential information provided by our business partners from information security incidents just as it does with the organization's own information assets.

Build on continuous improvement

DSG shall achieve sustainable information security management through continuous evaluation and revision of objectives set forth in DSG Information Security Policy.

第一三共グループ
情報セキュリティポリシー

第一三共株式会社

第一三共グループは、情報に対する適切な管理を重要な経営課題として認識し、情報セキュリティに関する基本方針を「第一三共グループ情報セキュリティポリシー（以下、本ポリシー)」として定めます。

- **CISO（Chief Information Security Officer）の設置**

  第一三共グループは、本ポリシーを有効にするためCISOを設置し、そのリーダーシップのもと、グローバルにおける情報セキュリティ対策を整備します。

- **情報セキュリティ管理体制の構築**

  第一三共グループは、保有するすべての情報資産の保護および適切な管理を行うため、CISOの指示のもとグループ各社に情報管理責任者を配置することで情報セキュリティ対策を速やかに実施できる体制を構築します。

- **社内規程の整備**

  第一三共グループは、情報セキュリティに関するグループ共通の社内規程を整備し、情報資産の保護、適切な管理を行うための方針・ルールを社内に周知・徹底します。

- **法令順守**

  第一三共グループは、情報資産に関する法令、規範およびお客さまとの情報セキュリティに関する契約上の要求事項･義務を遵守します。

- **適切な情報セキュリティ対策**

  第一三共グループは、情報資産に関する不正アクセス、情報漏えい、改ざん、破壊などの情報セキュリティ侵害を予防し、その被害を軽減するため、組織的・人的・物理的・技術的なセキュリティ対策に取り組みます。

- **情報セキュリティ意識の向上**

  第一三共グループは、すべての従業員等（当社の情報資産を利用するすべての利用者）に対して、情報セキュリティ意識の向上を図り、情報資産を適切に利用するための教育や訓練を継続的に実施します。

- **ビジネスパートナーへの対応**

  第一三共グループは、ビジネスパートナー における情報セキュリティへの取組みについて審査を行い、適切な情報セキュリティレベルを維持することを要請します。ビジネスパートナーと協力することで、当社の事業全体における情報セキュリティを高めます。

- **ビジネスパートナーの秘密情報への対応**

  第一三共グループは、ビジネスパートナーからお預かりした秘密情報についても当社の情報資産と同様に保護し、適切に取り扱います。

- **継続的改善の実施**

  第一三共グループは、上記の取組みを継続的に評価し見直しすることで、持続的な情報セキュリティマネジメントを実現します。

以上