資生堂グループ　情報セキュリティポリシー

本ポリシーは、資生堂グループ各社に勤務するすべての者（取締役、監査役、執行役、エグゼクティブオフィサー、従業員、出向社員、パート、アルバイトおよび派遣社員など。以下、あわせて「従業員等」という）を対象とし、資生堂グループ各社の情報資産の保護にかかわる規程（基準・ルール、関連規程・ガイドライン、各種運用マニュアル、およびその他の社内規則も含まれる。以下、あわせて「規程類」という）の基本ポリシーとして定められるものです。

I.　［ 目的 ］

本ポリシーは、資生堂グループ各社の情報資産および情報システムを不正使用、紛失、破壊、改ざん、漏えいおよび盗難等の各種のリスクから守るとともに、情報セキュリティの継続的な改善を通じて、企業価値の向上を図ることを目的とします。

II.　［ 定義 ］

1. 「資生堂グループ」とは、株式会社資生堂、その国内外の子会社および関連会社で構成される企業集団を指します。
2. 「資生堂グループ各社」とは、資生堂グループに帰属する各法人を指します。
3. 「情報資産」とは、紙または電磁的に記録された業務に関する一切の記録を指し、「機密情報」「個人情報」を含みます。
4. 「機密情報」とは、技術上、営業上、および経営上の情報で有用かつ公然と知られていない情報および第三者から守秘義務を負って取得した情報を指し、各国・地域の関係法令に基づき「機密情報」として保護されるべきものも含みます。
5. 「個人情報」とは、氏名、生年月日、住所、電話番号、画像、その他の記述等によって、特定の個人を識別できる情報を指し、各国・地域の関係法令に基づき「個人情報」として保護されるべきものも含みます。
6. 「情報システム」とは、コンピュータシステムを構成するハードウエア、ソフトウエアおよびネットワークを指します。
7. 「情報セキュリティ」とは、情報の可用性、機密性、完全性を確保することを目的とした、情報資産および情報システムの不正使用、紛失、破壊、改ざん、漏えいおよび盗難等の防止及び適正利用の遵守を指します。

III.　［ 情報セキュリティの推進体制 ］

1. チーフインフォメーションテクノロジーオフィサー（CITO）は、最高情報セキュリティ責任者として資生堂グループの情報セキュリティの遵守を通じて、情報資産と情報システムの取り扱いに関する包括的な責任を負います。また、資生堂グループ各社において機密情報管理・個人情報保護・情報システム管理・情報セキュリティ対策に関する規程類の整備および運用の徹底、安全対策の実施、教育訓練等の実践について監督を行います。
2. 各地域本社の代表者は、管轄地域内における情報資産と情報システムの取り扱いに関する管理責任者として、機密情報管理・個人情報保護・情報システム管理・情報セキュリティ対策に関する規程類の整備および運用の徹底、安全対策の実施、教育訓練等の情報セキュリティ全般に責任を負います。各地域本社の代表者は、管轄地域内における情報セキュリティの責任者を指名し、上記を推進させるものとします。
3. 資生堂グループ各社の各部門・事業所の責任者は、部門・事業所で取り扱う情報資産について、棚卸と保護、従業員等への教育訓練、取り扱い状況に関する自己点検、および事故発生時の対応等を行うものとします。
4. 情報セキュリティに関する会議体は、資生堂グループ全体の情報セキュリティへの取り組みを全グループにおける統一された意思のもと継続的に維持・向上させることを目的とし、定期的にまたは必要に応じ開催されます。

IV.　［ 委託先の管理 ］

1. 資生堂グループ各社は、各国・地域の法令の定義による個人情報の取り扱い、資生堂グループの規程類の定義による機密情報の取り扱い、および資生堂グループの業務の継続や品質の確保に大きくかかわると考えられる業務を、外部の取引先等に委託する場合、委託業務の遂行において情報セキュリティが確保されるよう、委託先に対する適切な管理・監督を行うとともに、資生堂グループの求める情報セキュリティ基準を満たすよう、必要に応じて安全管理措置の実施を求めています。

2. 1項の委託契約を締結する部門は、契約締結時、委託先の情報セキュリティ管理体制の確認を行います。また、契約締結後においても、委託する業務の内容を鑑みて、適切な時期や頻度を定め、情報セキュリティ管理体制の再確認を行います。
3. 1項の委託契約における委託先がさらに他社に再委託を行う場合、契約締結部門は、必要に応じ、委託先から事前に報告を行うよう求め、委託先が当該再委託先の情報セキュリティ管理体制について確認した内容や、委託先から当該再委託先に対する管理体制について、確認を行います。

V. [教育・点検・監視]

1. Ⅲ条の情報セキュリティの推進体制に基づき、資生堂グループ各社は、従業員等に対し本ポリシーを遵守するために適切な教育を定期的に実施し、従業員の意識向上を図ります。
2. Ⅲ条の情報セキュリティの推進体制に基づき、資生堂グループ各社は、機密情報管理・個人情報保護・情報システム管理・情報セキュリティ対策に関する点検を定期的に行い、不適切な取り扱いが発見されたときには是正措置を講じます。
3. Ⅲ条の情報セキュリティの推進体制に基づき、資生堂グループ各社は、情報資産および情報システム内のデータの正確性が保たれ、不正アクセス、改ざん、破壊から安全に保護されていること、承認されたユーザーのみがアクセスしていることを継続的に監視し、異常が発見されたときには是正措置を講じます。
4. Ⅲ条の情報セキュリティの推進体制に基づき、資生堂グループ各社は、情報資産および情報システムに関するサイバーリスクを継続的に監視し、事故が発生したときには迅速かつ適切な対応を行うとともに、関係法令および社内規程に基づき、適切かつ迅速に関係者への説明責任を果たします。

VI. [具体的な手続]

1. 資生堂グループ各社は、本ポリシーを遵守し、その目的を達成するために、各国・地域の関係法令に照らして必要な規程類を制定します。
2. 機密情報の管理方法等については、資生堂グループ各社が定める規程類において制定することとします。
3. 個人情報の管理方法等については、資生堂グループ各社共通の個人情報の取り扱いに関する基準である「資生堂グループ プライバシールール」を遵守するものとします。資生堂グループ各社は当該ルールおよび各国・地域の関係法令を遵守するための具体的手順を定めた規程類を制定することができます。

Ⅶ. [従業員等の義務]

1. 従業員等は、情報資産の保護の重要性を十分に認識した上で、法令、本ポリシー、および規程類を遵守し、情報資産の保護に努めなければなりません。
2. 従業員等は、情報資産の不正使用・紛失・破壊・改ざん・漏えい・盗難などの可能性がある場合、あるいはこれらの事案の発生を認識した場合には、直ちに社内の適切なレポートラインに報告し、また必要に応じて適用される現地法令の管轄当局に届け出なければなりません。
3. 従業員等は、上記1項・2項に違反した場合には規程類・就業規則、各種契約または関連法令等に基づき、解雇を含む懲戒処分の対象となることがあります。

Ⅷ. [情報セキュリティの継続的な改善]

1. 資生堂グループ各社は、情報資産および情報システムの保護水準を維持・向上させるため、情報セキュリティに関する取り組みを継続的に見直し、改善を図ります。
2. 情報セキュリティに関するリスクや脅威の変化、技術の進展、法令・規制の改正等に対応するため、必要に応じて規程類や運用体制の見直しを行います。
3. 教育・点検・監視の結果および事故の発生状況を踏まえ、再発防止策や改善策を講じることで、情報セキュリティの実効性を高めるよう努めます。

Ⅸ. [改廃]

本ポリシーの改廃は、株式会社資生堂の情報セキュリティ部門が起案し、株式会社資生堂の最高意思決定会議体の承認を

得るものとします。ただし、法令の改正に基づく改訂または事業への影響が軽微な改訂等については、CITO が決裁できるものとします。

■ 改訂履歴

2004 年 08 月 30 日制定
2011 年 06 月 15 日改定
2013 年 02 月 01 日改定
2016 年 04 月 01 日改定
2018 年 01 月 01 日全面改定
2021 年 11 月 15 日改定
2022 年 11 月 01 日改定
2024 年 3 月 26 日改定
2025 年 7 月 1 日改定