デリコ　情報セキュリティ基本方針

1. 目的

本情報セキュリティ基本方針(以下本基本方針と言う)は、株式会社デリコ(以下当社という)の情報セキュリティに関する基本方針を定めたものである。本基本方針は、当社及び当社がお預かりしているお客様ならびにお取引先の個人情報を含む情報資産を保護することを目的とする。

2. 対象範囲

本基本方針の対象範囲は、当社が業務で使用するすべての情報資産および情報資産を保全するための設備、更にこれらの情報資産を利用する当社の役員、社員、契約社員、アルバイトおよび派遣社員(以下全従業者という)とする。

3. 用語の定義

情報セキュリティ　：
　当社の事業継続を確実なものにすること、事業損害を最小限にすること、ならびに投資に対する見返りを最大限にすることを目的として、広範囲にわたる脅威から情報を保護すること。
情報セキュリティポリシー　：
　本基本方針。

4. 経営陣の意向表明

当社は、食と食をとりまく分野に幅広く挑戦し、食に関するネタ(情報等)を集め加工又は創造し、お客様と共に発展し続けることを目的としている。
この目的に則った企業活動を営むにあたり、当社固有の情報資産を活用すると共に、多くのお客様ならびにお取引先から情報資産をお預かりしている。
これらの情報資産に対し、当社は本基本方針に基づいて情報セキュリティを構築、運営し、必要な保護と適切な安全対策を講じる。
全従業者は、本基本方針を遵守し、情報セキュリティリスクを排除した安全な事業活動を通して、お客様に高い満足度を提供し、企業価値の拡大を図ることを目指す。

5. 基本方針

(1) 情報セキュリティポリシーの策定
当社経営陣の意向表明に従い情報セキュリティポリシーを策定し、全従業者へ周知徹底する。全従業者は、この情報セキュリティポリシーを遵守して情報セキュリティ対策を遂行する。

(2) 情報セキュリティ管理体制の確立
- 情報セキュリティに関して、全般的な責任を持つ情報セキュリティ管理責任者(以下管理責任者という)を設置する。管理責任者は、セキュリティ事件・事故に対応することを含め、情報セキュリティの構築・運営に関して組織を指導し、管理する責任を持つ。
- 全社レベルの情報セキュリティの状況を正確に把握し、必要な対策を迅速に実施できるようにするため、情報セキュリティ委員会を設置する。

(3) 見直し
経営環境の変化、社会環境や法規制の変化、情報関連技術の最新動向、および新たに発見されたリスクに照らし合わせて、本基本方針の適宜見直しを行い、継続的な改善を行う。

(4) 情報システム・セキュリティ対策の実施
当社情報システム資産を保護するために、リスク分析を実施し不正アクセス対策、ウイルス対策、漏洩対策、信頼性対策など情報システムに対するセキュリティ対策を実施する。

(5) 業務委託に関するセキュリティ対策

当社業務の外部委託について、会社機密情報および個人情報の保護の観点から、委託先の適格性の審査、契約書の内容に関する見直し、改善を図る。

(6) 法的および契約上の要求事項への適合
当社情報セキュリティに関連する法令、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるために、これらの要求事項を明確にして、適合するための対策を策定し実施する。

(7) 情報セキュリティに関する教育・訓練及び周知・徹底
全従業者に対し、定期的な情報セキュリティに関する教育・訓練を行い、情報セキュリティの重要性、適切な取り扱いおよび管理に関し周知・徹底を図る。

(8) セキュリティ事故への対応
情報セキュリティに関連する事故が発生した場合は、発見者は速やかに管理責任者にその内容を報告し、管理責任者は直ちに関係者に報告すると共に、必要に応じて緊急措置を講じることとする。これら情報セキュリティ事故については、その事故原因を分析し再発防止策を講じる。

(9) 事業継続管理
偶発的に発生する災害・故障・過失及び意図的に発生する情報資産の悪用などによる事業の中断を可能な限り抑え、事業の継続を確保する。

(10) 情報セキュリティポリシー違反に対する措置
当社社員が情報セキュリティポリシーに違反した場合は、懲戒手続きの対象とする。

2007 年 10 月 18 日

署名 前田正雄