はじめに

利益を生み出すための情報は非常に重要な資産であり、企業は社会的な責務として、想定できる多くの事故を未然に防がなければなりません。

そのため、私たちは、この情報セキュリティ基本方針書に基づき、想定できる事故の脅威から、情報資産を保護するための情報セキュリティ関連規則を作成し、統一された管理の下、諸施策を確実に実施、遵守するよう社員教育に勤め、皆様の信頼にお応えできるよう努めて参ります。

1. 目的

株式会社 アルス・ウェアー（以下、「当社」という）は、社内全般の管理業務および購買業務において、情報セキュリティの管理を実施する。

本情報セキュリティ基本方針書の設定目的は、顧客ならびに当社の情報資産をリスクから適切に保護し、想定しうる情報セキュリティ事故を未然に防止し、顧客に安全と安心を提供するために当社の役員、社員、協力会社社員、アルバイト、パートに情報資産保護の必要性と責任を公表・通知し徹底させることにある。

2. 情報セキュリティの定義

情報セキュリティとは、情報の機密性、完全性、及び可用性を維持することであり、場合によっては、真正性、責任追跡性、否認防止、及び信頼性のような特性を含むものとする。上記の業務を主たる業務とする当社にとって“情報セキュリティ”は、重要、且つ、最優先の課題であることを認識し、経営陣の陣頭指揮のもと積極的な取組みを行う。

3. 適用範囲

（1）本方針の適用範囲は、当社の管理する情報資産すべてとする。

（2）本方針における「情報」の範囲は、情報システム内に存在する電子的情報にとどまらず、文書、磁気媒体、端末画面、電話・FAXなどすべての形態を含む。

(3)本方針は、当社に所属するすべての役員、社員、協力会社社員、アルバイト、パートに適用される。

4. 情報セキュリティの目標

当社は以下を情報セキュリティの目標とする。

(1)適切な情報セキュリティ管理を実施し、情報セキュリティ事故を未然に防止し、情報セキュリティ事故の発生ゼロを目指す。

(2)万が一情報セキュリティ事故が発生した場合も、その被害を最小限にとどめ、迅速な復旧を行い、また再発を防止する。

(3)情報資産の可用性を確保し、必要な情報が必要なときに利用できるようにする。

5. 情報セキュリティ組織体制

当社の情報セキュリティに関する問題を検討、意思決定を行う機関として、最高責任者を代表取締役とし、代表取締役が任命する者により情報セキュリティ委員会を設置する。情報セキュリティ委員会は、組織別に部門セキュリティ担当を任命し設置する。

また、当社の情報セキュリティ管理が適切に行われていることを監査するため、代表取締役が内部監査責任者を任命する。

6. 情報セキュリティ原則

6.1 情報資産の管理

部門セキュリティ担当は、部門の情報資産を法令、契約および当社の定める情報セキュリティに関連する基準・手順に従い管理しなければならない。

6.2 情報資産に対する権限

部門セキュリティ担当は、情報資産に対する権限を与える際、業務上必要な者のみに必要な権限だけを与えるようにしなければならない。

6.3 情報資産の分類と対策の選択

部門セキュリティ担当は、情報資産をその重要性に応じて分類および管理しなければならない。なお、分類基準は事務局とCISOがその都度判断し、分類することとする。

6.4 監視

情報セキュリティ担当は、情報資産が適切に管理されていることを監視しなければならない。

6.5 監査方針および監査計画

以下の項目を監査方針とし、監査を行うこと。また、監査は定期的、計画的、継続的におこなうこと。

但し、不正摘発等については、機動的な監査を行うこと。

(1)情報セキュリティレベルを向上させる。

(2)顧客からの評価、セキュリティ改善要求などに迅速且つ適切に応える。

(3)セキュリティ対策の合理化および効果の向上を図る。

(4)役員、社員、協力会社社員、アルバイト、パートのセキュリティ意識を向上させる。

(5)情報セキュリティ事故の防止、発見および対応を改善する。

6.6 セキュリティ事件・事故の対応

情報セキュリティに関連する事件・事故が発生した場合、発見者は速やかに部門セキュリティ担当に

その内容を報告しなければならない。部門セキュリティ担当は情報セキュリティ委員会に報告し、情報セキュリティ委員会は、情報セキュリティに関連する事故原因の分析、再発防止策を講じなければならない。

6.7 事業継続管理

災害（自然災害、火災など）及びセキュリティ障害が発生した場合、事業への影響を最小限に抑え事業の継続を確保するため、事業継続管理の手順を明確に定めなければならない。

6.8 教育

情報セキュリティ委員長は、情報セキュリティに関する教育を計画し、当社の役員、社員および協力会社社員は、職務に応じて必要な情報セキュリティ教育を定期的に受け、”力量の向上”に努めなければならない。

6.9 各種規定の遵守

当社の役員、社員および協力会社社員は、情報セキュリティに関する基準・手順を遵守しなければならない。

6.10 法的および契約上の要求事項への準拠

当社の役員、社員および協力会社社員は、情報セキュリティ関連法令、契約などの要求事項を遵守しなければならない。

7. リスク評価基準

当社の管理する全ての情報資産について洗い出し、機密度、重要度および影響度などにより、情報資産に対するリスクの評価基準を設け、各情報資産が有するリスクを正しく評価すること。また、情報資産については、管理責任者を特定すること。

7.1 リスクアセスメントの体系的な取組方法

情報資産に対するリスクアセスメントを脅威および脆弱性の観点から起こり得るセキュリティ障害などの発生の可能性、情報資産に対する影響と管理策などを考慮し、ISMSの枠組みにおいて体系的に実施すること。

7.2 リスクの識別および管理策の適用

体系的なリスクアセスメントの結果に基づき、それぞれのリスクの性質・程度に応じて適切な管理策を適用し、情報セキュリティの確保・維持を図ることとする。適用した管理策は、「適用宣言書」により明確化する。

8. **レビュー**

本方針は経営方針の変更、事業内容の変更、社会的変化等が生じた場合、見直し、改善を行う。
また、法令の変更等を考慮し、定期的(年に1度)に見直しを行う。

9. **情報セキュリティ管理プロセス、管理策の有効性の測定**

“情報セキュリティ管理プロセス”、“リスクアセスメント”、“要求事項に対する管理策”、“情報セキュリティの監視、見直し”等について、定期的にその有効性の測定を行い、必要に応じて見直しを行わなければならない。

10. **周知**

本方針はすべての役員、社員、協力会社社員、アルバイト、パートに対して周知徹底する。

11. **処罰**

本方針および情報セキュリティに関する基準・手順、情報セキュリティ関連法令、契約などの要求事項に反するものは処罰の対象とする。

12. **本方針の施行**

本方針は、2008 年 9 月 1 日より施行する。
初版は 2008 年 9 月 1 日より施行する。
最終改訂日:2013 年 1 月 7 日

株式会社　アルス・ウェアー
東京都豊島区南池袋 2-29-12
メトロシティ南池袋ビル 7F
代表取締役　大友　孝昭