情報セキュリティ基本方針

株式会社カーリル

Version 1.0, 2019-07-09

基本声明

カーリルは、すべての情報資産に対する機密性、完全性、可用性の確保と向上に努め、図書館に求められる社会的要請に応えるため、情報セキュリティ基本方針（セキュリティポリシー）を定める。この方針に基づき情報セキュリティマネジメントシステムを確立し、継続的な情報セキュリティ対策を推進する。役員を含む全従業員がこの方針を理解し、遵守することを宣言する。

2019年7月9日

株式会社カーリル

代表取締役 吉本龍司

情報セキュリティの定義

情報セキュリティとは、機密性、完全性および可用性を確保し維持することをいう。

1. 機密性 (confidentiality): 情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
2. 完全性 (integrity): 情報が破壊、改ざんまたは消去されていない状態を確保すること
3. 可用性 (availability): 情報へのアクセスを認められた者が、必要時にアクセスできる状態を確保すること

適用範囲

- ウェブサービスの開発、運用およびサポート業務
- APIの開発、コンサルティング、運用およびサポート業務
- 本社施設とネットワーク
- 役員を含むすべての従業員（以下従業員とする）
- すべての情報資産

実施事項

1. 適用範囲の全ての情報資産を脅威（漏えい、不正アクセス、改ざん、紛失、破損、国家権力の濫用など）から保護するための情報セキュリティマネジメントシステムを確立、導入、運用、監視、見直し、維持および改善する。
2. 情報資産の取り扱いは、関係法令および契約上の要求事項を遵守する。
3. 重大な障害または災害により事業活動が中断しないように、予防および回復手順を策定し、定期的な見直しをする。
4. 情報セキュリティの教育・訓練を全従業員に対して定期的に実施する。

責任と義務

1. 情報セキュリティの責任は、代表取締役が負う。そのために代表取締役は、従業員が必要とする資源を提供する。
2. 従業員は、情報資産を守る義務がある。
3. 従業員は、本方針を維持するため策定された手順に従わなければならない。
4. 従業員は、情報セキュリティに関する事故および認知した脆弱性を報告する責任がある。
5. 本方針を維持するため策定された手順に故意または重大な過失により違反した従業員は、就業規則に従い処分する。

定期的見直し

情報セキュリティマネジメントシステムの見直しは、環境変化に合わせるため定期的に実施する。

改版履歴

- 2019年7月9日 制定（v1.0）