情報セキュリティ管理規程

(目的)

第１条　本規程は、株式会社ＲＩＣＯＳ（以下「当会社」という。）が業務上取り扱う顧客、取引先、および配分機関など（以下「顧客等」という。）の情報資産および当会社の情報資産を各種の脅威から適切に保護することにより、当会社の事業活動を正常かつ円滑に行うことを目的とする。

(用語の定義)

第２条　本規程における用語の定義は、次のとおりとする。

２　「従業者等」とは、会社の役員、従業員（労働契約法に基づいて労働契約を会社と締結した労働者をいう。）又は派遣労働者（労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律に基づく派遣労働者をいう。）をいう。

３　「情報資産」とは、情報、情報システム、およびこれらを適切に運用・管理・利用するために必要なものをいい、ハードウェア、ソフトウェア、ネットワークや記録媒体のほか、業務上知り得た情報、知識、ノウハウ等をすべて含むものとする。

４　「情報セキュリティポリシー」とは、「情報セキュリティに関する基本方針」および情報セキュリティに関する規程、規則をいう。

５　「情報セキュリティ」とは、情報資産の「機密性」、「可用性」および「完全性」を確保し、維持することをいう。

６　「機密性」とは、情報資産を、アクセス権限を持つ者のみに所定の方法にて開示し、アクセス権限を持たない者から保護することをいう。

７　「可用性」とは、情報資産を、アクセス権限を持つ者が必要なときに利用できるように保持することをいう。

８　「完全性」とは、情報資産を、整合性を保ちながら改ざん等がなされることなく、正確に処理し、保持することをいう。

(適用範囲)

第３条　本規程は、業務上取り扱う顧客等の情報資産および当会社の情報資産すべてに適用する。なお、顧客等の情報資産の管理・取扱い等について、契約や規程等により特段の運用ルール等を定めている場合には、当該運用ルール等に従うものとする。

２　個人情報に関わる保護については、当会社で別途定めているプライバシーポリシーに従うものとする。

３　本規程は、前項の情報資産を利用する従業員等に適用する。

(情報セキュリティ管理委員会)

第４条　当会社は、情報セキュリティに関する統括組織として、情報セキュリティ管理委員会を設置する。

２　情報セキュリティ管理委員会は、情報セキュリティポリシーに基づく情報セキュリティの徹底を推進するとともに、情報セキュリティに関し情報セキュリティポリシーに定めのない事項についての判断基準を示す等、当会社における情報セキュリティ全般につき統括する。

３　情報セキュリティ管理委員会の委員長は代表取締役とし、総務部を事務局とする。

４　情報セキュリティ管理委員会は、必要に応じて関連担当部門と連携のうえ任務を遂行するものと

する。

5　情報セキュリティ管理委員会は、委員長の任命した者を情報管理責任者とし、必要に応じて情報セキュリティの状況を確認させることができるものとする。

(情報管理責任者)

第５条　情報管理責任者は、情報セキュリティ管理委員会委員長を補佐し、組織内の情報セキュリティにつき責を負うとともに、当該組織内における指導・啓蒙や適切な環境の整備等、情報セキュリティポリシーを徹底するために必要な措置を講じるものとする。

(教育研修責任者)

第６条　教育研修責任者、情報セキュリティポリシーに定められた事項を理解・遵守するとともに、従業員等に情報セキュリティポリシーを遵守させるための教育を企画・運営する責任を負うものとする。

(システム点検責任者)

第７条　システム点検責任者は、情報セキュリティポリシーに定められた事項を理解・遵守するとともに、定期的に情報セキュリティポリシーが遵守されているかを監査する責任を負うものとする。

(情報へのアクセス管理)

第８条　当会社に属する情報は、従業員等が必要な期間・必要な範囲でのみアクセス権限を有することとする。ただし、新たに登録すべき従業員等の更新などの場合には、情報管理責任者が必要と認めた範囲内の情報を必要と認められた者のみが、情報管理責任者の管理下においてアクセスすることができる。

2　顧客等に属する情報は、情報取扱者以外の者が、機微情報に接したり、職務上、提供を要求してはならない。

3　顧客等が承認した場合を除き、一切の事業者以外の者（親会社、地域統括会社等の事業者に対して指導、監督、業務支援、助言、監査等を行う者を含む）に対して、機微情報を伝達又は漏えいしてはならない。

4　電子化情報を当会社内で保管する場合は、アクセス制限された電算システム内に保管することとし、当該アクセスのためパスワードはアクセスを許可された本人および情報管理責任者のみに付与され、何人にも教えてはならない。

5　非電子化情報を当会社内で保管する場合は、入退室が制限された部屋において、施錠されたロッカー内に保管することとし、当該ロッカーの鍵は情報セキュリティ管理委員会委員長及び情報管理責任者が各１つずつ保有し、何人にも貸与してはならない。

(情報の返却・廃棄)

第９条　従業員等は、不必要となった機密情報を直ちに返却又は廃棄しなければならない。

2　従業員等は、記録媒体を問わず、機密情報を不必要に複写してはならない。

(教育の実施)

第１０条　教育研修責任者は、全社員に情報セキュリティポリシーを遵守させるための教育を企画・運営するものとする。なお、教育の内容およびスケジュール等は、事業年度ごとに教育研修責任者が定めるものとする。

(リスク評価)

第１１条　情報セキュリティ管理委員会は、技術の進歩や業務環境の変化等も考慮のうえ、情報資産のリス

ク評価を多方面から継続的に実施し、それを情報セキュリティポリシーおよびそれに基づく各種施策に反映させることにより、情報セキュリティの維持・向上を図るものとする。

(点検の実施)

第１２条　システム監査責任者は、情報セキュリティポリシーの遵守状況を定期的に監査するものとする。

2　システム監査責任者より情報セキュリティポリシーの遵守状況につき改善、勧告等を受けた被監査部門は、改善計画書を作成のうえ、適切な是正措置を講じなければならないものとする。

(緊急対応)

第１３条　全ての従業員等は、情報セキュリティ上の問題が生じた場合又は発生する恐れがある場合には、直ちに情報管理責任者に報告するものとする。情報セキュリティ上の問題には、再生が必要な情報の喪失、漏えい及び改ざんが含まれる。

2　当該報告を受けた情報管理責任者は、直ちに情報セキュリティ管理委員会を設定して、当該問題を報告する。

3　情報セキュリティ管理委員会は、速やかに問題の解決策を検討し、情報管理責任者をその実施にあたらせる。

(違反した場合の措置)

第１４条　従業員等が情報セキュリティポリシーに違反した場合は、当会社の就業規則に基づき懲戒に処す。

2　派遣社員および協力社員が情報セキュリティポリシーに違反した場合は、派遣元または業務委託先との契約に従うものとする。

附則　この規程は、令和５年２月１日から施行する。