1　情報セキュリティポリシー

浅利観光株式会社（以下、当社）では、宿泊、コワーキングスペースの利用を通じて、地域産業の貢献を図るとともに、テレワークの安心・安全を取り扱う事業者として、情報セキュリティおよび個人情報保護を含むコンプライアンスの徹底が企業活動の原点であるという認識のもと、情報セキュリティ推進体制の整備・強化に努めます。

従業員等は、本情報セキュリティポリシー（以下、本ポリシー）を理解・順守のうえ、業務を遂行することを誓います。

（基本原則）

・お客様に関する情報は適切に収集し、管理・維持します。また、当社が社外へ委託する情報についても適正に管理・維持します。
・順守すべき法令、規制コンプライアンスを徹底します。
・当社が定めた規程類、委託先等との情報セキュリティ締結事項を順守します。
・情報セキュリティに関する管理体制を構築し、情報セキュリティ対策の継続的な改善・見直しを実施します。
・情報資産のセキュリティリスクを適切に評価し、その結果を考慮して効果的なセキュリティ対策を推進します。
・万一、情報漏洩等のセキュリティ事故や事業継続に支障をきたす事象が発生した場合には、迅速な是正措置を実施するとともに、当社の事業に関連する利害関係者にその状況を報告します。
・情報セキュリティおよび個人情報保護に関して、従業員等の知識とモラルの向上を図り、企業利益の維持・向上および顧客満足のために、徹底した情報セキュリティレベルの確保と順守に努めます。
・当社の情報セキュリティが適切に対策されているか、定期的に確認を行います。

当社は、本ポリシーに従い、常に社会からの信頼を得る必要があることを十分に認識するとともに、商品の安全・安心と適正な情報セキュリティ管理に真摯な姿勢で臨むことを、ここに宣誓します。

2　定義

情報資産とは、社内外を問わず当社の経営・事業に係るすべての情報とし、研究開発・営業・企画・手法等の技術およびノウハウ、サービス、取引先情報、契約情報、会社設備、従業員等の情報に係るものについて、電子記録による情報､文書により記録された情報等、記録媒体の形態を問わないものである。
情報セキュリティは事業活動の継続を阻害しないよう、情報資産が不正等による脅威からの保護、資産価値（機密性・完全性・可用性（下記「表 2-1 資産価値」を参照））の確保と維持により、事業継続のための適切な対策が施されることである。

表 2-1 資産価値

機密性（漏れる）	漏洩・流出・盗聴 / サーバ不正利用・侵入 / 盗難
完全性（変わる）	改ざん・混入 / サーバ誤処理 / 改変・改造 / 損失・破壊
可用性（消える・戻せない・使えない）	損失・破壊 / サーバ停止

3　対象範囲

- 当社の事業活動に関わる全ての情報資産および従業員等を対象とする。
- 従業員等は、情報セキュリティおよび個人情報の取扱いに関する誓約書に署名しなければならない。
- 取引先等の第三者に情報を開示する必要がある場合には、情報開示に関する契約を締結しなければならない。

4　従業員等の責務

従業員等は、情報セキュリティの重要性について認識を持つとともに、情報資産の利用にあたっては目的外の利用を禁止とし、本ポリシーを順守するものとする。

また、本ポリシーに違反した者は、就業規則に従い懲戒処分等の対象となる場合がある。派遣社員および外部委託者等が、本規程に違反した場合は、契約またはその他の取決めに従う。

5　推進・管理体制

- 情報セキュリティに関する統括組織として、経営者および各部門長が、会社の情報セキュリティに関する施策全般の管理・運営・推進を行う。
- 各部門長は、本ポリシーの趣旨を理解し、実践できるよう全ての従業員等に周知徹底し、定期的に情報セキュリティ教育・訓練を行い、順守状況を評価する。
- 経営者は、情報セキュリティに関する規定・対策・その他の諸規則を承認するとともに、当社の情報セキュリティを統括する。
- 経営者は、情報セキュリティの責任に関する方針、自らの関与の明示、責任の明確な割当ておよび承認を行う。
- 各部門長は、重要な情報資産の把握と区画管理を行い、権限を有しない者の利用を試みさせてはならない。
- 従業員等は、権限のない情報資産を不正に入手してはならない。また、入手した情報資産を使用し不正行為を行ってはならない。
- 関係当局（行政機関、規制当局、通信事業者等）や情報セキュリティに関する研究会または会議、および情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。
- 情報セキュリティおよびその実施のマネジメントに対する組織の取組み（例えば、情報セキュリティのための管理目的、管理策、ポリシー、プロセス、手順）は、あらかじめ定期的に、必要に応じてレビューを実施する。
- 本ポリシーに定めのない、別の組織体制および職務分掌については、別途、関連規程類で定めるものと

する。

6　情報セキュリティ体制

情報セキュリティポリシーの実効性を確保するため、以下の情報セキュリティ対策を講ずる。

6.1　人的セキュリティ対策

本ポリシーの趣旨を理解し、実践できるよう、従業員等に周知徹底を行い、盗難、不正行為、または施設の不正使用等のリスクを低減するため、定期的な情報セキュリティ教育・訓練を行う。

当社の従業員等の雇用にあたって、経歴等の確認を、関連のある法令、規則および倫理に従って行い、個人の責任および組織の責任を記載した雇用契約書に同意し、署名する。休職時・退職時には、情報資産の不正利用や紛失、当社外への流出等を防止するために、すべてのアクセス権限を失効するとともに、貸与・供与した情報資産の返却・滅失を適時実施する。経営者および各部門長は別途規程に定めている、保持する権限や役職によって、守秘義務を記した誓約書等の署名を取得する。

6.2　物理的セキュリティ対策

当社拠点・設備への不正侵入、情報資産の盗難・改ざん・破壊等の危険にさらされることのないよう、各拠点・設備への入退室及びサーバや通信機器等の装置・機器等の物理的管理において対策を講ずる。

（物理設計）

オフィス、セキュリティルーム等の IT 環境を利用・設置する建物または設備は、火災・地震等の自然災害や、不正なアクセスによる情報機器の盗難、紛失、破壊を防ぐために、物理的防御や入退館制限等の必要な管理をする。

（付帯設備）

当社に関るすべての施設は、施設に関る付帯設備（電気、空調等）を適切に管理・保守を行う。

（物理配線）

物理配線を流れるデータの傍受による情報漏洩や、物理配線の破壊・破損による情報の消失等を防止するために、物理配線は適切に管理・保守を実施する。

（情報機器および媒体）

情報機器および媒体は、施錠可能な部屋に設置し適切な管理を行う。また、火災・地震等の自然災害からの影響を考慮し、設置場所を選定する。

6.3　技術的セキュリティ対策

情報資産を参照・利用するための権限を定め、業務上正当な必要性を有する者のみがアクセス可能な環境を構築する。また、情報資産への不正アクセスや当社外への情報資産の流出を防止するために、アクセス制御やコンピュータウィルス対策等の施策を実施する。

（アクセス制御）

第三者からの不正なアクセスを防ぐために、侵入防止、ネットワークの分離、接続制御、アクセス経路の統一等の適切な管理を行う。従業員等は、許可された情報機器から、本人認証を行った上で IT 環境へアクセスする。

（電子メール）

社内外との情報交換の手段として、電子メールを利用する場合は情報漏洩、紛失等のリスクを考慮し、交換される情報の重要度によって、暗号化技術（パスワード等）を使用する等、情報の機密性および完全性を維持するために必要な管理策を実施する。

（コンピュータウィルス対策）

コンピュータウィルス等のマルウェアの実行を防ぐために、会社から提供されたウイルス対応ソフトを適切に運用し、感染防止に努める。コンピュータウィルスを検知した場合は、直ちに感染防止措置を取り、システム部門へ報告する。

（脆弱性対策）

管理部門は、所管する情報システム（OS、パッケージソフトウェア含む）の脆弱性情報を適宜収集し、必要と認められる場合は、従業員等に周知および作業指示を行う。

6.4　緊急時対策

自然災害や情報システム不具合、機器故障、不正行為といった不測の事態により、当社の事業活動が中断・停止しないよう、適切な予防措置を講ずる。

6.5　事故対応

万一、当社の事業活動が中断または停止する事象が発生した場合には、定められた連絡体制に基づき、直ちに所属上長および関係者、関係部署（社）へ報告し、速やかな原因究明と拡大防止、再発防止策の立案、実施に努めると同時に、当社の事業に関連する利害関係者にその状況を報告する。

7　個人情報

個人情報保護ポリシーおよび個人情報保護規程等に従い、適切な管理を行う。

8　法令および各種規範の順守

当社事業において情報セキュリティに関連する法令、基準、ガイドライン等を含む要求事項および契約に対する違反を避けるため、常に関連する法令等を確認し、最新の状態に保つ手順を明確にする。

当社に適用される情報セキュリティ上の管理策の追加、変更、廃止等により、法的要求事項に対応しなければならない事象が発生した場合には、必要に応じて、組織の法律顧問等の専門家に法的な助言を求める。

経営者および各部門長は従業員等に対し、関連法令に関する教育を行い、各適用法令に従った適切な対応と情報保護および記録保管を実施する。

9　教育・評価・監査による見直し

当社の従業員等に本ポリシーの順守状況を検証するために、定期的に、必要に応じて教育と評価を行い、各部門に対して監査を行う。

監査の結果から情報セキュリティ体制・対策の有効性評価を実施し、あわせて本ポリシーの見直しを実施するものとする。

以上

2022 年 9 月 1 日制定
浅利観光株式会社　代表取締役　植田　裕一