大項目	中項目	小項目	要求事項（管理策）	回答
5 セキュリティ基本方針	5.1 情報セキュリティ基本方針	5.1.1 情報セキュリティ基本方針文書	情報セキュリティ基本方針文書は，経営陣によって承認され，全従業員及び関連する外部関係者に公表し，通知することが望ましい。	当社の情報セキュリティ基本方針は、以下で公開しております。 https://www.shanon.co.jp/security/
		5.1.2 情報セキュリティ基本方針のレビュー	情報セキュリティ基本方針は，あらかじめ定められた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当及び有効であることを確実にするためにレビューすることが望ましい。	当社では、ISMS のプロセスに基づき、定期的にレビューを実施しております。直近の見直し日は 2026年10月19日 です。
6 情報セキュリティのための組織	6.1 内部組織	6.1.1 情報セキュリティに対する経営陣の責任	経営陣は，情報セキュリティの責任に関する明りょうな方向づけ，自らの関与の明示，責任の明確な割当て及び承認を通して，組織内におけるセキュリティを積極的に支持することが望ましい。	ISMS のプロセスに基づき、情報セキュリティマネジメントシステムに関するリーダーシップを発揮し、継続的に取り組んでおります。
		6.1.2 情報セキュリティの調整	情報セキュリティ活動は，組織の中の，関連する役割及び職務機能をもつ様々な部署の代表が，調整することが望ましい。	ISMS のプロセスに基づき、情報セキュリティに関する責任者および各部門の担当者を明確にし、必要に応じて部門横断の調整や連携を行う体制を整えております。また、情報セキュリティ教育も継続的に実施しております。
		6.1.3 情報セキュリティ責任の割当て	すべての情報セキュリティ責任を，明確に定めることが望ましい。	ISMS のプロセスに基づき、役割と責任を明確に定義しております。お客様との責任範囲についても、SHANON MAIL 利用規約において明示しております。
		6.1.4 情報処理設備の認可プロセス	新しい情報処理設備に対する経営陣による認可プロセスを定め，実施することが望ましい。	ISMS の規程に基づき、当社が利用する情報処理設備やサービスの導入時には、リスク評価および承認プロセスを経て適切に認可する運用としております。
		6.1.5 秘密保持契約	情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューすることが望ましい。	SHANON MAIL 利用規約にて秘密保持に関する内容を定めております。本サービスは無償で提供されるため、個別の秘密保持契約（NDA）の締結には対応しておりません。個別の締結を必要とされる場合は、有償プラン（SHANON MA）のご利用をご検討ください。
		6.1.6 関係当局との連絡	関係当局との適切な連絡体制を維持することが望ましい。	緊急連絡体制を整備し、社内および社外の関係当局との連絡体制を維持しております。
		6.1.7 専門組織との連絡	情報セキュリティに関する研究会又は会議，及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ことが望ましい。	情報セキュリティに関する専門業者との連絡体制を維持しております。
		6.1.8 情報セキュリティの独立したレビュー	情報セキュリティ及びその実施のマネジメントに対する組織の取組みについて，あらかじめ計画した間隔で，又はセキュリティの実施に重大な変化が生じた場合に，独立したレビューを実施することが望ましい。	ISMS のプロセスに基づき、独立したレビューを定期的に実施しております。
	6.2 外部組織	6.2.1 外部組織に関係したリスクの識別	外部組織がかかわる業務プロセスからの，組織の情報及び情報処理施設に対するリスクを識別し，また，外部組織にアクセスを許可する前に適切な管理策を実施することが望ましい。	SHANON MAIL 利用規約にて当社とお客様の責任範囲を明示しております。
		6.2.2 顧客対応におけるセキュリティ	顧客に組織の情報又は資産へのアクセスを許す前に，明確にしたすべてのセキュリティ要求事項を満たすように対処することが望ましい。	セキュリティに関する情報は当社ウェブサイトにて公開しており、SHANON MAIL 利用規約に沿って情報を開示しております。
		6.2.3 第三者との契約におけるセキュリティ	組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約，又は情報処理施設に製品・サービスを追加する第三者との契約は，関連するすべてのセキュリティ要求事項を取り上げることが望ましい。	当社がクラウドサービスや外部委託先を利用する場合、ISMS の規程に基づき、契約時に情報セキュリティ要件を確認し、必要な管理策が満たされていることを確認しております。また、契約後も必要に応じてセキュリティ要件の遵守状況を確認し、適切な管理が継続されていることを評価しております。本サービスの提供に関する業務を再委託する場合は、再委託先に対し、利用規約所定の当社の義務と同等の義務を負わせております。なお、本サービスの生成AI機能において外部の生成AIサービス（外国にある事業者が提供するものを含みます）を利用する場合、当社は当該事業者との間で、入力情報および生成物を当該事業者のAIモデルの学習に利用しない旨を確認したうえで利用しております。
7 資産の管理	7.1 資産に対する責任	7.1.1 資産目録	すべての資産を明確に識別し，また，重要な資産すべての目録を作成し，維持することが望ましい。	ISMS に基づき、情報資産を識別し資産管理台帳として記録・管理しております。また、サービス内のデータについては利用状況を確認できる機能を提供し、資産把握を補完しております。
		7.1.2 資産の管理責任者	情報及び情報処理施設と関連する資産のすべてについて，組織の中に，その管理責任者を指定することが望ましい。	本サービスに登録された情報（リード情報等）の利用権限はお客様に帰属します。SHANON MAIL 利用規約にて明記しております。ただし当社は、同規約に定める範囲において契約者データを利用いたします。
		7.1.3 資産利用の許容範囲	情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。	本サービスに登録された情報の利用権限はお客様に帰属します。当社による契約者データの利用目的および範囲は SHANON MAIL 利用規約に明記しており、当社従業員についても ISMS 規程に基づきデータ利用の許容範囲を定め、遵守させております。
	7.2 情報の分類	7.2.1 分類の指針	情報は，組織に対しての価値，法的要求事項，取扱いに慎重を要する度合い及び重要性の観点から分類することが望ましい。	SHANON MAIL 利用規約および当社プライバシーポリシーにおいて明示しております。
		7.2.2 情報のラベル付け及び取扱い	情報に対するラベル付け及び取扱いに関する適切な一連の手順は，組織が採用した分類体系に従って策定し，実施することが望ましい。	ISMS に基づき、情報資産を機密区分ごとに分類し、分類に応じた取扱いルールを定めております。
8 人的資源のセキュリティ	8.1 雇用前	8.1.1 役割及び責任	従業員，契約相手及び第三者の利用者のセキュリティの役割及び責任は，組織の情報セキュリティ基本方針に従って定め，文書化することが望ましい。	ISMS 規程に従い、情報セキュリティの観点での役割及び責任を定めております。
		8.1.2 選考	従業員，契約相手及び第三者の利用者のすべての候補者についての経歴などの確認は，関連のある法令，規則及び倫理に従って行うことが望ましい。また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行われることが望ましい。	採用選考においては、ISMS の規程に基づき、業務に必要な信頼性および適性を確認するプロセスを設けております。
		8.1.3 雇用条件	従業員，契約相手及び第三者の利用者は，契約上の義務の一部として，情報セキュリティに関する，これらの者の責任及び組織の責任を記載した雇用契約書に同意し，署名することが望ましい。	雇用契約および就業規則には、情報セキュリティに関する義務、秘密保持、データ取扱いに関する事項を明記しております。また、ISMS に基づく追加規程についても、入社時に説明し、理解と遵守を求めております。

※ 本資料は SHANON MAIL（無償）について記載したものです。有償プラン（SHANON MA）とは提供内容および保証水準が異なります。