はじめに及び概要

第 1.1 条　はじめに

1.1.1 AudioCodes Ltd.（以下「当社」といいます。）は、サービスプロバイダー及び企業向けに、高度な Voice-over-IP（VoIP）技術並びに VoIP 及びデータネットワーキングの融合製品及びアプリケーションを設計、開発、販売しております。当社は、VoIP 技術分野における市場のリーダーとして、VoIP 及びデータ通信の融合に注力しており、当社製品は、ブロードバンド、モバイル、ケーブル及び企業ネットワーク等、世界各国のネットワークにおいて導入されております（以下「本サービス」といいます。）。

1.1.2 本ポリシーは、当社が取得したデータ、特に個人データの保護及び安全管理の方法を定めることを目的として作成されたものです。

1.1.3 本ポリシーにおいて、「AudioCodes」とは、AudioCodes Ltd.及びその「関連会社」を意味し、ここでいう「関連会社」とは、子会社、親会社、共同事業体その他の共通の所有権の下にある法人を指します。

第 1.2 条　定義

1.2.1「データ管理者」
個人データの取扱いの目的および手段を単独または他者と共同で決定する自然人または法人、公的機関、機関その他の団体をいう。かかる取扱いの目的および手段が EU 法または加盟国法により定められている場合には、当該管理者またはその指名に関する特定の基準は、EU 法または加盟国法により定められることがある。

1.2.2「データ処理者」
管理者のために個人データを処理する自然人または法人、公的機関、機関その他の団体をいう。

1.2.3「データ対象者」
管理者または処理者により個人データが処理される自然人をいう。

1.2.4「識別可能な自然人」
氏名、識別番号、位置情報、オンライン識別子、または当該自然人の身体的、生理的、遺伝的、

精神的、経済的、文化的、社会的な特性に特有の一つ以上の要素を参照することにより、直接的または間接的に識別され得る者をいう。

1.2.5「個人データ」
識別された、または識別可能な自然人（「データ対象者」）に関するあらゆる情報をいう。識別可能な自然人とは、氏名、識別番号、位置情報、オンライン識別子、または身体的、生理的、遺伝的、精神的、経済的、文化的、社会的な特性に特有の一つ以上の要素を参照することにより、直接的または間接的に識別され得る者をいう。

第 1.3 条　目的および適用範囲

1.3.1 本ポリシーは、AudioCodes 社が、組織内、業務提携先および子会社における情報の機密性、完全性および可用性に影響を及ぼすリスク、特に個人データに関連するリスクを管理することに対する責任と取組みを定めるものである。

1.3.2 本ポリシーは、以下に定める原則に基づき策定されるガイドライン、基準、業務プロセスおよび手続等の詳細なデータ保護および情報セキュリティに関する文書の基礎となるものである。

第 1.4 条　適用対象

1.4.1 本ポリシーは、AudioCodes 社の情報資産の取扱いに関与するすべての AudioCodes 社の従業員および供給業者に対して適用され、当該者は本ポリシーを遵守し、これを実施する責任および義務を負うものとする。

第 2 条　情報セキュリティに関する役割および責任

第 2.1 条　　経営陣

経営陣は、企業統治全体に対して最終的な責任を負うものとする。データ保護および情報セキュリティに関するリスクの管理および統制は、企業統治の不可欠な要素である。具体的な責任は以下のとおりとする。

2.1.1　データ保護および情報セキュリティに関する方針ならびに情報セキュリティ目標が、組織の戦略的方向性と整合するように策定されていることを確保すること。
2.1.2　情報セキュリティに関するパフォーマンス指標およびインシデントに関する報告を受領し、これに対応すること。

2.1.3 情報セキュリティマネジメントシステム（ISMS）の要件が組織の業務プロセスに統合されていることを確保すること。
2.1.4 情報セキュリティマネジメントシステムの運用に必要な資源が確保されていることを保証すること。
2.1.5 情報セキュリティマネジメントの有効性および ISMS 要件の遵守の重要性を組織内に周知徹底すること。
2.1.6 情報セキュリティマネジメントシステムがその目的を達成することを確保すること。
2.1.7 AudioCodes 社の経営陣は、情報セキュリティ運営委員会としての役割を担い、当該委員会は少なくとも年 1 回開催され、期間中に提起された主要な課題について審議・承認を行うものとする。

第 2.2 条 最高情報セキュリティ責任者（CISO）

AudioCodes 社の CISO（最高情報セキュリティ責任者）は、以下の事項について全般的な責任を負うものとする。

2.2.1 AudioCodes 社の製品およびソリューションに関する情報セキュリティの確保。
2.2.2 AudioCodes 社の開発ライフサイクル全般（企画、分析、設計、試験および実装を含む）におけるセキュリティ関連事項の監督。
2.2.3 安全なソフトウェア開発ライフサイクル（Secure Software Development Lifecycle）の実施に関する方針および手続の策定。
2.2.4 すべての開発者およびサポートチームが、安全なソリューションを提供するために必要な知識および理解を有することの確保。
2.2.5 AudioCodes 社の情報セキュリティリスクの評価および情報セキュリティプログラムの設計。
2.2.6 セキュリティ計画およびセキュリティリスクを AudioCodes 社の経営陣に報告し、リスクに基づく意思決定の基礎とすること。
2.2.7 AudioCodes 社のセキュリティプログラムの策定、維持および監督。
2.2.8 適用されるすべての情報セキュリティ要件に対応するための方針、プロセスおよび統制手法の策定、維持および監督。

2.2.9 情報セキュリティの確立および維持を継続的に監督すること。
2.2.10 情報セキュリティに関連する課題および懸念事項について、組織に対して助言を行うこと。
2.2.11 情報セキュリティインシデントの対応を調整すること。

2.2.12　情報セキュリティプログラムの運用に関する調整およびフォローアップを行うこと。
2.2.13　定期的なコンプライアンスレビューを実施し、すべてのシステムに対するユーザーアクセスの再認証を含むこと。

第 2.3 条　データプライバシー管理責任者

データプライバシー管理責任者は、プライバシー運営委員会の一員として、漏えい対応および通知、データ保護影響評価（DPIA）、その他のプライバシー関連事項を含む方針およびプログラムの改善に関する提言を行うものとする。当該委員会には、IT 部門、法務部門、IT セキュリティ部門の代表者および必要に応じてその他の構成員が含まれるものとする。

AudioCodes 社のデータプライバシー管理責任者は、以下の事項について全般的な責任を負うものとする。

2.3.1　GDPR およびその他のプライバシー関連法令に基づく義務について、AudioCodes 社および個人情報の取扱いを行う従業員に対して通知および助言を行うこと。
2.3.2　プライバシー関連法令および AudioCodes 社の個人データ保護に関する方針の遵守状況を監視すること（責任の割当、関係者への啓発および教育、ならびに関連する監査を含む）。
2.3.3　データ保護影響評価に関する助言を求められた場合にはこれを提供し、その実施状況を監視すること。
2.3.4　監督機関との協力を行うこと。
2.3.5　個人情報の取扱いに関する事項について、監督機関との連絡窓口としての役割を果たすこと。

第 2.4 条　IT マネージャー

IT チームは、プロダクション環境におけるネットワーク、システムおよびデータの安全な構成を確保する責任を負うものとする。

IT チームマネージャーの責任は、以下のとおりとする。

2.4.1　プロダクション環境における情報資産の機密性、完全性および可用性を保護するため、適切な保護措置を実施すること。
2.4.2　プロダクション環境における情報資産の一貫した保存、処理および送信を確保するため、管理および運用手順を文書化し、周知すること。

2.4.3　アクセス権の付与および剥奪を管理し、セキュリティリスクを把握・報告し、それらがプロダクション環境における情報資産の機密性、完全性および可用性に与える影響を理解すること。

第 2.5 条　従業員および契約社員

すべての従業員および契約社員は、以下の事項を遵守すべきものとする

2.5.1　情報資産の保護に関する方針、ガイドラインおよび手続に従うこと。
2.5.2　情報セキュリティまたは方針違反の事実またはその疑いがある場合には、CISO（最高情報セキュリティ責任者）およびデータプライバシー管理責任者に報告すること。
2.5.3　情報漏えいの事実またはその疑いがある場合には、CISO に報告するとともに、個人データに関する漏えいについてはデータプライバシー管理責任者にも報告すること。

第 3 条　リスクベースの情報セキュリティプログラム

AudioCodes 社の情報セキュリティプログラムは、リスクマネジメントの実践に基づいて構築されるものとする。情報セキュリティリスクマネジメントプロセスを定義し、以下の目的のために適用する。

3.1.1　計画された間隔で、または重要な変更が提案された場合または発生した場合に、情報セキュリティリスク評価を実施すること。
3.1.2　新技術を使用する場合で、自然人の権利および自由に対して高いリスクが生じる可能性があるときは、AudioCodes 社は、想定される処理活動が個人データの保護に与える影響を評価するため、データ保護影響評価（DPIA）を実施するものとする。
3.1.3　リスク評価の結果を踏まえ、適切な情報セキュリティリスク対応策を選定すること。
3.1.4　選定された情報セキュリティリスク対応策を実施するために必要な統制措置を決定すること。
3.1.5　情報セキュリティリスク対応計画を策定すること。
3.1.6　情報セキュリティリスク対応計画に対するリスク所有者の承認および残存する情報セキュリティリスクの受容を取得すること。

第 4 条　AudioCodes 社のデータ保護および情報セキュリティに関する基本原則

第 4.1 条 人的資源

4.1.1　AudioCodes 社は、従業員、契約社員、業務提携先およびベンダーが、自らのデータ保護およびセキュリティに関する責任を理解するよう確保するものとする。

4.1.2　組織のすべての従業員および、必要に応じて契約社員に対して、職務に関連する範囲で、適切な意識向上教育および研修、ならびに組織の方針および手続に関する定期的な更新を実施するものとする。

第 4.2 条　資産管理および処理活動記録

4.2.1　AudioCodes 社は、物理的および地理的な所在にかかわらず、すべての情報資産のインベントリ（資産台帳）を維持するものとする。すべての資産は分類され、必要に応じて暗号化やハードニング（堅牢化）を含む適切な保護レベルが確保されるものとする。
4.2.2　処理活動記録の維持の一環として、AudioCodes 社は、業務プロセスに関与する個人データをマッピングし、データ主体のカテゴリおよび個人データのカテゴリ（人種、政治的意見、宗教、性的指向、遺伝情報、生体情報、児童に関する情報などの特別カテゴリを含むがこれに限られない）を記述するものとする。

第 4.3 条 アクセス制御

4.3.1　AudioCodes 社は、情報資産および個人データへのアクセスが、認可されたユーザーのみに限定されるよう確保するものとする。ユーザーには、明示的に認可された資産へのアクセスのみが付与されるものとする。

第 4.4 条　暗号技術の利用

情報の機密性、真正性および完全性を保護するために、暗号技術を適切かつ効果的に利用することを目的として、AudioCodes 社は以下を確保するものとする。

4.4.1　第三者に対してデータを送信する際には、会社のデータ分類方針に従い、安全なプロトコルを用いて移動中のデータを暗号化するものとする。

第 4.5 条　物理的および環境的セキュリティ

4.5.1　AudioCodes 社は、組織の情報および情報処理施設に対する不正な物理的アクセス、損害および妨害を防止するため、物理的および環境的な対策を講じるものとする。

第 4.6 条　運用および通信のセキュリティ

4.6.1　AudioCodes 社は、IT プロダクションの管理に関する変更管理、キャパシティ管理、マルウェア対策、バックアップ、ログ管理、監視および脆弱性管理を含む適切な統制措置を維持するものとする。
4.6.2　AudioCodes 社は、ネットワークセキュリティ、ネットワークの分離、ネットワークサービス、情報の転送および安全なメッセージ通信を含む通信セキュリティに関する適切な統制措置を維持するものとする。

第 4.7 条　システムの取得、開発および保守

4.7.1　AudioCodes 社は、情報システムのライフサイクル全体にわたりセキュリティを維持するものとする。
4.7.2　AudioCodes 社は、システムまたはソフトウェアの分析および設計の段階においてセキュリティおよびプライバシーを考慮し、データ最小化などのデータ保護原則を効果的に実施するための適切な措置を講じ、処理に必要な保護措置を統合することにより、データ主体の権利を保護する（設計および初期設定によるデータ保護）。
4.7.3　適切なセキュリティレベルの評価にあたっては、特に、処理により生じ得る偶発的または違法な破壊、喪失、改ざん、不正な開示またはアクセスのリスクを考慮するものとする。
4.7.4　AudioCodes 社は、処理のセキュリティを確保するための技術的および組織的措置の有効性を定期的に試験、評価および査定するプロセスを実施するものとする。

第 4.8 条　サプライヤーとの関係

4.8.1　AudioCodes 社は、契約、定期的な監査および必要な措置を通じて、業務提携先、供給業者および契約業者が、AudioCodes 社の顧客情報を保護するために十分なセキュリティ対策を維持することを確保するものとする。

第 4.9 条　情報セキュリティインシデントの管理

4.9.1　AudioCodes 社は、すべての従業員が情報セキュリティインシデントの発生を未然に防止するよう努めることを確保するものとする。万が一インシデントが発生した場合には、「個人データ漏えい対応方針」に基づき、速やかに適切な措置を講じるものとする。
4.9.2　個人情報が漏えいまたは毀損されたプライバシー侵害が発生した場合には、AudioCodes

社が当該事実を認識してから 72 時間以内に、所轄の監督機関に対して通知を行うものとする。

4.9.3　データ主体に重大な損害を及ぼすおそれのあるプライバシー侵害が発生した場合には、データ主体に対しても、遅滞なく通知を行うものとする。

第 4.10 条　コンプライアンス

4.10.1　AudioCodes 社は、契約上、規制上および法令上の遵守義務を特定し、必要に応じてこれらを情報セキュリティプログラムに統合するものとする。

4.10.2　AudioCodes 社は、一般データ保護規則（GDPR）等の関連法令および最善のセキュリティ実務に従うことを約束する。

4.10.3　AudioCodes 社は、情報セキュリティマネジメントシステムの有効性に関する情報を得るため、計画的な間隔で内部監査を実施するものとする。