1. Introduction & Overview

1.1. Introduction

1.1.1. AudioCodes Ltd. designs, develops and sells advanced Voice-over-IP (VoIP) and converged VoIP and Data networking products and applications to service providers and enterprises. AudioCodes is a VoIP technology market leader focused on converged VoIP & data communications and its products are deployed globally in broadband, mobile, cable, and enterprise networks (the "Service").

1.1.2. This Policy has been created to define the ways in which AudioCodes protects and secures data, specifically personal data provided to it.

1.1.3. In this Policy, "AudioCodes" refers to AudioCodes Ltd. and its "Affiliates", which shall mean subsidiaries, parent companies, joint ventures and other corporate entities under common ownership.

1.2. Definitions

1.2.1. "Data Controller" - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

1.2.2. "Data Processor" - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

1.2.3. "Data Subject" - a natural person whose personal data is processed by a controller or processor

1.2.4. "Identifiable natural person" - means one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.2.5. "Personal Data" - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

1.3. Purpose and Scope

1.3.1. This policy establishes AudioCodes' commitment to manage the risks affecting the confidentiality, integrity and availability of information within the organization, business partners and subsidiaries, specifically those related to personal data.

1.3.2. This policy serves as the foundation for detailed data protection and security documentation such as guidelines, standards, processes and procedures based on the principles outlined below.

1.4. Applicability

1.4.1. All AudioCodes personnel and suppliers, who are involved with AudioCodes' information assets, are responsible and accountable for adhering to and implementing this policy.

2. Information Security Roles and Responsibilities

2.1. Senior Management

Senior Management are ultimately accountable for corporate governance as a whole. The management and control of data protection and information security risks is an integral part of corporate governance. Specific responsibilities include:

2.1.1. Ensure that the data protection and information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
2.1.2. Receive and act upon information security performance metrics and information security incidents;
2.1.3. Ensure the integration of the information security management system requirements into the organization's processes;
2.1.4. Ensure that the resources needed for the information security management system are available;
2.1.5. Communicate the importance of effective information security management and of conforming to the information security management system requirements;
2.1.6. Ensure that the information security management system achieves its intended outcome(s);
2.1.7. AudioCodes senior management acts as the Information Security Steering Committee. This forum meets at least annually, reviews and approves the AudioCodes security program, and discusses major information security issues raised during this period.

2.2. Chief Information Security Officer (CISO)

AudioCodes CISO has the overall responsibility for:

2.2.1. Ensuring the information security of AudioCodes products and solutions;
2.2.2. Overseeing security aspects in all AudioCodes development lifecycle including planning, analysis, design, testing and implementation;
2.2.3. Developing policies and procedures for implementing Secure Software Development Lifecycle;
2.2.4. Ensure that all developers and support teams have the required knowledge and understanding for supplying secure solutions.
2.2.5. Assess AudioCodes information security risks and design the information security program;
2.2.6. Communicate the security plan and security risks to AudioCodes management as a basis for risk based decisions;
2.2.7. Develop, maintain and oversee AudioCodes security programs;
2.2.8. Develop, maintain and oversee policies, processes and control techniques to address all applicable information security requirements;

2.2.9. Oversee the establishment and maintenance of information security on a continuous basis;
2.2.10. Advise the organization of information security related issues and concerns;
2.2.11. Coordinate the handling of information security incidents;
2.2.12. Coordinate and follow-up on the operation of the information security program;
2.2.13. Perform periodic compliance reviews, including recertification of users access to all systems;

2.3. Data Privacy Manager

The Data privacy Manager should be part of a privacy steering committee, providing recommendations to improve policies and program initiatives including breach response and notification, Data Protection Impact Assessments, and other privacy matters. The committee should include members representing IT, Legal, IT Security and other members as needed.

AudioCodes Data privacy Manager has the overall responsibility to:

2.3.1. Inform and advise AudioCodes and the employees who carry out processing of personal information of their obligations pursuant to GDPR and to other privacy regulations;
2.3.2. Monitor compliance with privacy regulations and with the policies of AudioCodes in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits;
2.3.3. Provide advice where requested regarding the data protection impact assessment and monitor its performance;
2.3.4. Cooperate with the supervisory authority;
2.3.5. Act as the contact point for the supervisory authority on issues relating to processing.

2.4. The IT Manager

The IT team is responsible for ensuring secure configuration of the network, systems and data in the production environment.

The IT Team Manager's responsibilities include the following:

2.4.1. Implement appropriate safeguards to protect the confidentiality, integrity and availability of information assets in the production environment;
2.4.2. Document and disseminate administrative and operational procedures to ensure consistent storage, processing and transmission of information assets in the production environment;
2.4.3. Provision and de-provision access; understand and report security risks and how they impact the confidentiality, integrity and availability of information assets in the production environment.

2.5. All Employees and Contractors

All employees and contractors should:

2.5.1. Adhere to policies, guidelines and procedures pertaining to the protection of information assets.
2.5.2. Report actual or suspected security and/or policy violations to the CISO and Data privacy Manager.
2.5.3. Report actual or suspected breaches to the CISO and those involving personal data to the Data privacy Manager as well.

3. Risk Based Information Security Program

AudioCodes information security program will be based on a risk management practice. We define and apply an information security risk management process to:

3.1.1. Perform information security risk assessments at planned intervals or when significant changes are proposed or occur.
3.1.2. Where using new technologies, and where it is likely to result in a high risk to the rights and freedoms of natural persons, AudioCodes will carry out a Data Protection Impact Assessment (DPIA) to determine the impact of the envisaged processing operations on the protection of personal data.
3.1.3. Select appropriate information security risk treatment options, taking in account the risk assessment results;
3.1.4. Determine controls that are necessary to implement the information security risk treatment options chosen;
3.1.5. Formulate an information security risk treatment plan;
3.1.6. Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

4. AudioCodes' Data Protection and Information Security Principles

4.1. Human Resources

4.1.1. AudioCodes will ensure that employees, contractors, partners and vendors understand their data protection and security responsibilities.

4.1.2. All employees of the organization and where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

4.2. Asset Management and Records of Processing Activities

4.2.1. AudioCodes will maintain an inventory of all its information assets, regardless of its physical and geographical location. All assets will be classified, to ensure that all information receives appropriate level of protection, including encryption and hardening where required.

4.2.2. As part of the maintenance of the Records of Processing Activities, AudioCodes will map the private data involved within its processes including a description of the categories of data subjects and of the categories of personal data (including, but not limited to special categories of personal data, e.g. a person's race, political opinions, religion, sexuality, genetic info, biometrics, children information)

4.3. Access Control

4.3.1. AudioCodes will ensure that only authorized users will have access to its information assets and to private data.

4.3.2. Users will only be provided with access to assets that they have been specifically authorized to use.

4.4. Cryptography

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, AudioCodes will ensure that:

4.4.1. Data in motion will be encrypted using secure protocols when transmitted to 3rd parties, in accordance with the company data classification policy.

4.5. Physical and Environmental Security

4.5.1. AudioCodes will use physical and environmental measures to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

4.6. Operational & Communication Security

4.6.1. AudioCodes will maintain appropriate controls related to management of IT production including change management, capacity management, malware, backup, logging, monitoring and vulnerabilities management.

4.6.2. AudioCodes will maintain appropriate controls related communication security including network security, segregation, network services, transfer of information and secure messaging.

4.7. System acquisition, development and maintenance

4.7.1. AudioCodes will maintain security throughout the lifecycle of the information systems.

4.7.2. AudioCodes will consider security and privacy during system or software analysis and design and will implement appropriate measures, designed to implement data-protection principles, such as data minimization, in an effective manner and will integrate the necessary safeguards into the processing in order to protect the rights of data subjects. (Data protection by Design and by Default).

4.7.3. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

4.7.4. AudioCodes will implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

4.8. Supplier Relationship

4.8.1. AudioCodes will ensure that its partners, suppliers and contractors will maintain adequate security measurements to secure AudioCodes and its customers' information, through contracts and periodic audits as necessary.

4.9. Information Security Incident Management

4.9.1. AudioCodes will ensure that all employees work to prevent information security incidents from occurring. Should an incident take place, AudioCodes will swiftly implement appropriate actions as documented in the Handling Personal Data Breaches policy.

4.9.2. In the event of privacy breaches that have exposed or damaged personal information, the proper authorities will be notified within 72 hours of AudioCodes becoming aware of them.

4.9.3. In the event of privacy breaches that carry a high risk of harm to data subjects, the data subjects will be notified without undue delay.

4.10. Compliance

4.10.1. AudioCodes will identify compliance requirements, including contractual, regulatory and legal requirements, and integrate them into the Information Security Program as necessary.

4.10.2. AudioCodes is committed to comply with best security practices and relevant regulations such as General Data Protection Regulation (GDPR).

4.10.3. AudioCodes will conduct internal audits at planned intervals to provide information on the effectiveness of the information security management system.