Pexip Security and Privacy Policy

Document Owner	Chief Executive Officer
Document Classification	Public
Document Version	2.2 – 7 December 2023

Purpose

This document sets out the information security and privacy policy, affirms the direction, principles, and basic rules for information security and privacy management at Pexip.
This document is based on guidance from ISO/IEC 27002:2017 and ISO/IEC 27003:2017.

Scope

This document applies to all Pexip personnel, all Pexip information processing facilities and all Pexip information assets. The audience for this document is the Pexip workforce and interested parties to the ISMS seeking to understand Pexip's policy on information security and privacy.

Objective

Ensure the confidentiality, integrity and availability of information and information processing facilities within our care.

Policy

Why?

We are all responsible for protecting the privacy and ensuring the security (Confidentiality, Integrity, and Availability) of information and intellectual property at Pexip. Equally important: We want to deserve the trust that our customers, partners, and others extend to us.

How?

At Pexip, we approach information security aligned with our company cultural value, defined by:

- One Team
- No Bullshit
- Professional & Fun
- Freedom and Responsibility

The Details

At Pexip, protecting the privacy and ensuring the security of information resources is part of everyone's job. Our partners, customers, employees, and others rely on us to protect their information. An information breach could severely damage our credibility, result in financial and operational risk, and create regulatory compliance problems. Privacy and security events can also cause loss of business and other harm to our organisation. Strong information security requires diligence by all workforce members, including employees, contractors, consultants, interns, and any other authorised party accessing or using our information assets.

This policy promotes an effective balance between information security practices and business needs. This policy helps our organisation meet our legal obligations and the expectations of our partners and customers. Accordingly, Pexip commits that it will:

- comply with applicable privacy and data protection laws;

- balance the need for business efficiency with the need to protect sensitive, proprietary, or other confidential information from undue risk;
- grant access to sensitive, proprietary, or other confidential information only to those with a need to know and at the least level of privilege necessary to perform their assigned functions;
- become and remain in full compliance with the requirements of the ISO/IEC 27001:2013 and 27701:2019 standard;
- document our compliance-related activities and efforts, in accordance with the documentation requirements of the ISO/IEC 27001:2013 and 27701:2019;
- manage and maintain compliance-related documentation per required document retention periods, in accordance with Pexip's document retention policy; and
- Implement, maintain and improve the technical and organisational security and privacy measures necessary to deliver products and services to our customers with the appropriate level of security.

Recognising that a competent workforce is the best line of defence, we will provide security training opportunities and expert resources to help individuals understand and meet their information security obligations.

Managing Information Security

Effective Measures and Intended Outcomes

Pexip measures the fulfilment of its privacy and security objectives. The measurements must be performed at least once a year and the measurement results will be analysed, evaluated, and reported to the senior leadership as part of the management review. Intended outcomes of this management system are as follows:

- manage security and privacy risks through a methodology for identifying threats, identifying vulnerabilities, and implementing mitigations;
- protect supply chain assurance;
- illustrate evidence of best practices, demonstrating credibility and competence when tendering for contracts;
- minimize financial loss, protecting Pexip from destructive threats;
- improve processes through integrating the appropriate security measures in the operating procedures of the company to ensure they are consistent, repeatable and maintainable in day to day execution. promote continual improvement, through a re-evaluation annually;
- meet regulatory compliance with laws and regulations internationally; and

Objectives and Effective Measures

The objectives and effective measures of our ISMS are determined by the stakeholders of the management system and approved by the senior management

Changes to our objectives and effective measures may be proposed during management review meetings of the ISMS & PIMS or when the situation requires possible changes.

Information Security & Privacy Requirements

Pexip is required to maintain compliance with ISO/IEC 27001:2013 and 27701:2019 standard, its policies, contractual agreements with its customers and legal and regulatory obligations relevant to the organisation in the field of information security and personal data protection.

Legal & Regulatory Compliance

Various information security and data protection laws, regulations and industry standards apply to Pexip and the data we handle. Pexip is committed to complying with applicable laws, regulations, and standards.

Pexip maintains a record of laws and regulations applicable to Pexip as it relates to data privacy and data protection, both in terms of geographic and sectoral application. Pexip also maintains a global data breach notification matrix and contact information for the supervisory authorities in each territory where it operates.

Risk Management

Pexip utilises a combination of both qualitative and quantitative risk assessment model and has a documented procedure for the assessment and treatment of its risks.

Risk decisions are made based on the requirements of interested parties and the risk level to the organisation.

Information Security Controls

Pexip commits to enacting, supporting, and maintaining information security controls, as required by the standard, or as required to reduce risk to the business and our partners, customers, and end users.

Pexip identifies controls to reduce the risk levels of assets requiring treatment. Control objectives and controls may be selected from any suitable source but are always compared to the controls offered in Annex A of ISO/IEC 27001:2013, 27017:2015, 27018:2019 and 27701:2019. All control objectives and controls are documented in Pexip's Statement of Applicability.

Pexip maintains its Statement of Applicability, which identifies the information security and privacy controls that have been selected for our management system along with their implementation status. Controls and their objectives are selected during the management of risk.

Change Management

Pexip is an agile company that takes pride in challenges brought about by internal and external changes. Technical or organisational changes that have or may have significant impact on Pexip's information security or privacy practices or outcome are managed based on the assessed risk level.

Responsibilities

It is the responsibility of the Pexip senior leadership to assign information security roles and responsibilities at Pexip and to ensure that personnel understand their role. The key roles and responsibilities for information security are defined and documented in our ISMS Manual.

Communication

The Pexip senior leadership, in collaboration with department managers, ensure Pexip's workforce and appropriate interested parties are familiar with its information security and privacy policies.

Support

The Pexip senior leadership are committed to the implementation, management and continual improvement of information security and privacy program and ensure that adequate resources are available to support these objectives as an integrated part of the operating procedures of the company .

Enforcement

Non-Compliance

Intentional violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals may be subject to loss of provisioned information resources access privileges.

Exceptions

Any exception to this policy must be approved by the document owner in advance.

Review

This document will be reviewed annually and updated to reflect the findings of the review. It will also be reviewed following a major incident which requires a review of this document, and or a major change which impacts this document.