]pexip[

Pexip Services and the UK's NCSC 14 Cloud Security Principles

The UK's National Cyber Security Centre has specified 14 Cloud Security Principles to inform organisations about how to configure, implement and operate cloud services in a secure manner.

This whitepaper reflects safeguards employed in the context of these 14 Cloud Service Principles when using the Pexip service.

PEXIP AS | OSLO, NORWAY | AUGUST 2020

Table of contents

ABSTRACT

This whitepaper delineates the security and privacy practices employed by Pexip to secure customer data when using the Pexip cloud service or the Pexip Infinity platform in the context of the National Cyber Security Centre's 14 Cloud Security Principles (CPSs). The information provided within this briefing aims to articulate the particularities of Pexip's security praxis, providing customer confidence

and assurance in the security posture employed throughout Pexip's culture and operational environment.

INTRODUCTION

Pexip specializes in unified communications and collaboration (UC&C) meeting solutions, providing UC&C services for voice, video, content sharing, chat. Interoperable with Microsoft Teams, Google and other UC&C services, the scalable solution is available as both a cloud service or an on-prem virtualized infrastructure platform, powering a ubiquitous experience across mobile, desktop and conference room endpoints. Pexip is the result of a 2018 merger between two symbiotic Oslo-based companies (Videxio and Pexip).

Pexip's meeting solutions are available in flexible deployment models designed to meet the unique privacy and security requirements of enterprises and industry.

- Pexip-as-a-Service refers to Pexip's cloud solution for hosted meetings. It is available to enterprises on a subscription basis. In this deployment model, Pexip is responsible for the network and infrastructure.

- Customer Managed Virtualized Dedicated Platform refers to Pexip's customer-managed solution. Customers may deploy Pexip's virtualized infrastructure platform in a preferred cloud instance. For example, customers with existing subscriptions to Microsoft Azure, AWS or Google Cloud Platform may deploy and run Pexip within the cloud of choice, including both private and public clouds.

- Customer Hosted Virtualized Dedicated Platform refers to Pexip's customer-managed and hosted solution. Customers may deploy Pexip's virtualized infrastructure in data centres. When running as a self-hosted application, Pexip does not require an Internet connection to -hosted function; in this deployment model and for the ultimate in privacy, customers may choose to deploy a completely self platform only accessible from a private network. In this deployment model the customer is responsible for the network and infrastructure.

Deployment Model	Who administrates the service?	Who manages?	Who is hosting?
Pexip-as-a-Service	Customer	Pexip	Pexip
Customer Managed	Customer	Customer	Cloud provider[1]
Customer Hosted and Managed	Customer	Customer	Customer

Throughout this document, the context refers to Pexip-as-a-Service unless otherwise denoted.

Security and Compliance Practices at Pexip

Pexip is committed to upholding high standards of information security, privacy and transparency for its customers, partners and employees. The company offers security-first, enterprise-grade video conferencing solutions using industry-standard encryption and security protocols to maintain privacy and security. Compliance and certifications of the Pexip solution include:

- GDPR (Regulation EU 2016/679) compliance; and
- ISO/IEC 27001:2013 certification.

The Pexip security and compliance group has implemented and maintains an Information Security Management System (ISMS) according to the ISO/IEC 27001:2013 standard and audited by DNV GL. This means:

- Pexip has formalised internal information security best practices and implemented the practices from the ISO/IEC 27001:2013 standard.
- Pexip has formalised a management review of the information security management system and its performance.
- Pexip meets the requirements of relevant regulatory, contractual, and other legal obligations.
- Pexip is committed to meeting regulatory compliance with international laws and demonstrates worldwide recognition of excellence by employing an international framework with specific codes of practice.

[1] Cloud providers, in this scenario, provide the hosting. Examples are Azure, AWS, and GCP.

- Pexip is committed to proactively testing both the software solution and service to ensure they do not introduce any attack vectors to customer networks.

Objectives of this Document

The purpose of this publication is to convey transparently the security practices of the organisation and its services in the context of the United Kingdom's 14 Cloud Security Principles.

How to Read this Document

The remainder of this document is divided into fourteen sections, one section for each of the NCSC's 14 Cloud Security Principles. The sections are organized as follows:

NCSC Cloud Security Principle

The primary section header identifies the cloud security principle covered within the section by title and principle number.

Goals and Objectives of the Principle

NCSC defined objectives the implementation should achieve.

Pexip Responsibility

Details of how Pexip implements the principle within its service.

Customer Responsibility

Populated when a customer has responsibility for implementing the control.

PRINCIPLE 1: DATA IN TRANSIT PROTECTION

NCSC Guidance: User data transiting networks should be adequately protected against tampering and eavesdropping. The NCSC advises this should be accomplished through several mechanisms such as network protection and encryption.

- network protection - denying your attacker the ability to intercept data
- encryption - denying your attacker the ability to read data

Goals/Objectives

You should be sufficiently confident that:

- data in transit is protected between end user device(s) and the service;
- data in transit is protected internally within the service; and
- data in transit is protected between the service and other services (e.g. where APIs are exposed).

These goals are accomplished through the following Pexip responsibilities.

Pexip Responsibility

All communication links between Pexip's management nodes and conferencing nodes (and between individual conferencing nodes) employ IPsec transport with the following settings:

- 256-bit AES CBC-mode encryption;
- SHA 512 hashing for integrity validation; and
- a 4096-bit Diffie-Hellman modulus for key exchange.

No other ciphers, hashes or moduli are permitted. These settings apply to both the initial channel set-up for key exchange (ISAKMP) and the secondary channel over which application data is transported (ESP).

Inter-node traffic is restricted to only protocols that are expected for the successful operation of Pexip Infinity, including but not necessarily limited to call signalling, media, status, and configuration information; any unexpected traffic or protocols are dropped.

Encrypted connections between Pexip and external video conferencing endpoints use the following settings:

- AES 128-bit or 256-bit encryption for media, depending endpoint support;
- TLS for SIP call control (for more information, see managing TLS and trusted CA certificates);
- SRTP for SIP media; and
- H.235 for H.323 media.

WebRTC or the Pexip soft client (formerly My Meeting Video, used with web/desktop/mobile) clients employ the following protocols:

- HTTPS TLS for signalling; and
- DTLS-SRTP for WebRTC media.

Customer Responsibility

When a customer dials into a Pexip virtual meeting room (VMR) using legacy hardware that does not support encryption or deprecated levels of TLS (such as TLS 1.0 or TLS 1.1), the customer assumes the risk of a man-in-the-middle attack. It is advised that the customer upgrade firmware/hardware to support updated protocols and encryption modules.

Note:[2] In relation to dedicated platform deployments, client and administrative facing interfaces can be deployed into customers data centres or cloud compute behind customer firewalls for customer-controlled network transport protection and control. For more information, see how encryption is used for data in transit: https://docs.pexip.com/admin/encryption_methodologies.htm

PRINCIPLE 2: ASSET PROTECTION AND RESILIENCE

NCSC Guidance: User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure. The NCSC advises organisations to consider the following areas of safety regarding asset protection and resilience:

- physical location and legal jurisdiction;
- data centre security;
- data at rest protection;

[2] The guidance in this publication refers to Pexip-as-a-Service, a SaaS cloud implementation. This document may occasionally provide guidance regarding on-prem deployments, as in this case, where such a deployment forms a private cloud instance.

- data sanitisation;
- equipment disposal; and
- physical resilience and availability.

Each of these practice areas are described below.

Physical Location and Legal Jurisdiction

NCSC Guidance: That NCSC recommends service providers disclose the locations where data is stored, processed and managed and to delineate the legal circumstances under which data can be accessed without your consent. It also recommends the importance of knowing how data-handling controls within the service are enforced relative to UK legislation.

Goals/Objectives:

According to NCSC guidance, the user should understand:

- In which countries your data will be stored, processed and managed. You should also consider how this affects your compliance with relevant legislation such as the Data Protection Act 2018 (DPA).
- Whether the legal jurisdiction(s) within which the service provider operates are acceptable to you.

Pexip Responsibility

Pexip processes data in 18 data centre locations according to the data protection regulations commensurate with local laws. Beyond geographic regulations, Pexip complies with many sectoral regulations such as those related to healthcare, finance and others.

The physical locations of Pexip's data centres and/or offices are as follows: San Jose, CA, US; Ashburn, VA; Miami, FL; Toronto, CA; Sao Paulo, BR; London; Amsterdam (2); Frankfurt; Oslo (2); Johannesburg; Singapore (2); Hong Kong; Tokyo (2); and Sydney (2). Pexip provides for continuity of operations by implementing redundant services within each data centre facility and supports geographic redundancy by supporting data centre failover to mitigate against service localised disruption.

Pexip leverages subprocessors to provide the best experience and service to partners, end customers, and end users when using our video-conference products and services or when visiting our websites. A subprocessor is a third-party data processor engaged by Pexip, who has or potentially will have

access to service data or personal data. For example, Mailchimp is one of the subprocessors, used whenever Pexip sends a service announcement about feature enhancements or an upcoming update. Pexip engages different types of subprocessors to perform various processing functions. A list of current and previous subprocessors is available for review here.

The Pexip security and compliance group evaluates the security, privacy and confidentiality practices of prospective subprocessors before employing them. In doing this, Pexip ensures subprocessors meets the rigorous requisites of contractual obligations and statutory duties according to its responsibilities to data controllers.

Pexip's privacy notice describes the personal data that might be processed when using the Pexip products or services, and how it is protected.

Customer Responsibility

Prior to subscribing to Pexip's service, customers should read Pexip's privacy notice and list of approved subprocessors to determine the legal jurisdictions within which we as the service provider process their service data and personal data in the context of the service. Customers should follow the Pexip subprocessors support article to ensure they receive updates on changes to subprocessors.

Data Centre Security

NCSC Guidance: Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.

Goals/Objectives

You should be confident that the physical security measures employed by the provider are sufficient for your intended use of the service.

Pexip Responsibility

Pexip information systems are co-located in geographically dispersed data centres. Agreements with these data centre providers are covered by virtue of contractual agreements, which specify baseline security requirements in accordance to ISO/IEC 27001:2013 or SSAE-18 SOC2 requirements. Pexip's information security policies require data centre suppliers to meet and or exceed these baseline security requirements.

Pexip maintains a published list of data centre service locations on its support site located here. Pexip audits its data centre providers annually, keeping record of each supplier's evidence of practice.

Evidence is reviewed and updated at minimum annually to ensure that all providers maintain compliance. The provision and management of the information systems hosted within these data centres and the logical access are Pexip's responsibility, whilst the physical security is the responsibility of the data centre provider.

Data at Rest Protection

NCSC Guidance: Service providers should ensure data is not available to unauthorised parties with physical access to infrastructure; service providers should also ensure user data held within the service is protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.

Goals/Objectives

Provide sufficient confidence to customers that storage media containing their data are protected from unauthorised access.

Pexip Responsibility

Pexip has implemented a multi-layered approach to protecting data at rest within its service. These approaches include:

- Logical access controls, including:
    - role based access controls;
    - multifactor authentication; and
    - employment and enforcement of strong passwords.
- Network segmentation, ensuring separation of service and management networks.
- Encryption, ensuring:
    - backup data is encrypted;
    - Pexip portable computing devices and storage devices with service data is encrypted;
    - databases with service data are encrypted.

Within the Pexip cloud, data at rest is protected using AES-256 encryption. Voice, video and content sharing media are not stored, but transit through systems real-time. Please see the Data Processing Addendum in Annex A for a list of data collected, stored, processed and transferred through Pexip's cloud system, including the lawful basis of processing as well as the purpose, nature and types of data processed.

Data Sanitisation

NCSC Guidance: The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data. Inadequate sanitisation of data could result in:

- your data being retained by the service provider indefinitely;
- your data being accessible to other users of the service as resources are reused; and
- your data being lost or disclosed on discarded, lost or stolen media.

Goals/Objectives

Customers should be confident that data is erased when resources are moved or re-provisioned, when they leave the service or when they request it to be erased. Customers should be confident that storage media which has held their data is sanitised or securely destroyed at the end of its life.

Pexip Responsibility

Pexip's information classification policy specifies the methodologies used to sanitise information from storage media and its data retention procedure specifies when the methodologies are carried out. Pexip's data retention policies ensure call detail records are summarised when they age beyond 24 months. The detailed call logs are no longer retrievable after that timeframe, only high-level transaction summaries. When subscribers terminate use of the service, information is likewise summarised after 24 months.

Pexip employs three classification levels of information disposal and is used under varying circumstances according to its policies and procedures: erasing, clearing, and purging.

- Erasing: When performing a deletion process against a file, media erasure may be sufficient for Pexip lower-end erasures of confidential content.
    - Diagnostic support data is held for no more than 90 days and then erased.
- Clearing. The process of clearing is akin to overwriting—preparing media for reuse and assuring data cannot be recovered by employing traditional tools. Cleared data means information is overwritten with other content, such as a single character or a bit pattern. This process is employed with portable media.
    - Service log data is cleared every 90 days.
- Purging. Beyond clearing is the process of purging, an intense form of clearing providing assurance that the original data is not recoverable using any known methods. Purging

combines degaussing plus clearing for magnetic media, starting with clearing and ending with degaussing to completely remove the data. This process can be used with backup systems when applicable.

- Customer data is purged within 90 days following request for deletion or 6 months following the conclusion of processing.

Equipment Disposal

NCSC Guidance: Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.

Goals/Objectives

You should be sufficiently confident that:

- All equipment potentially containing your data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled).
- Any components containing sensitive data are sanitised, removed or destroyed as appropriate.
- Accounts or credentials specific to redundant equipment are revoked to reduce their value to an attacker.

Pexip Responsibility

Hardware assets within the scope of service delivery that have reached end of life are destroyed using one of the following methods:

- crushing,
- shredding,
- incinerating,
- disintegration, or
- dissolving using caustic or acidic chemicals.

Third-party destruction services are used when employing these methods, resulting in a certificate of destruction. This especially includes memory elements that are associated with production services or operations services. The Information Security Management System contains policy and practices regarding equipment disposal triggers and accountability.

Physical Resilience and Availability

NCSC Guidance: Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on a customer's business.

Goals/Objectives

Customers should be sufficiently confident that the availability commitments of the service, including their ability to recover from outages, meets their business needs.

Pexip Responsibility

Pexip's service is designed and built with multiple layers of resilience and redundancy.

- dual power supplies
- redundant power feeds
- dual network cards
- dual network feeds
- dual power suppliers
- high availability

By employing these N+1 redundancy within each data centre, and by employing data centre failover in the event of a localised issue, Pexip is able to maintain high-availability services on a global scale.

Note: In relation to on-prem deployments, the customer owns the data, the access and determines the deployment locations.

PRINCIPLE 3: SEPARATION BETWEEN USERS

NCSC Guidance: A malicious or compromised user of the service should not be able to affect the service or data of another. This is true where factors may affect user separation, including:

- where the separation controls are implemented as this is heavily influenced by the service model (e.g. IaaS, PaaS, SaaS);
- who you are sharing the service with - this is dictated by the deployment model (e.g. public, private or community cloud); and

- the level of assurance available in the implementation of separation controls.

Goals/Objectives

The following goals are noted in association with Principle 3.

- Ensure customers understand the types of users with whom with whom they share the service or platform.
- Ensure the service provides sufficient separation of customer data and service from other users of the service.
- Ensure customer management of the service is kept separate from other users.,

Pexip Responsibility

Pexip's service is a multi-tenant Software-as-a-Service (SaaS) deployed as a community cloud. The hierarchy of how users are organised follows a parent/child model and utilises logical separation at the database level. Pexip provisions partners to the service. Partners are the children of Pexip, they resell the service to customers. Customers are the children of the partner who provisioned them.

Customer Responsibility

It is the customer's responsibility to employ the administrative portal to manage users including the associated privileges in regard to organisational access and privilege level.

Note: In relation to dedicated platform deployments, the customer data is completely separated from other customers.

PRINCIPLE 4: GOVERNANCE FRAMEWORK

NCSC Guidance: The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments and the appearance of new threats.

Goals/Objectives

You should have sufficient confidence that the service has a governance framework and processes which are appropriate for your intended use. Good governance will typically provide:

- A clearly identified, and named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title ‘Chief Security Officer’, ‘Chief Information Officer’ or ‘Chief Technical Officer’.
- A documented framework for security governance, with policies governing key aspects of information security relevant to the service.
- Security and information security are part of the service provider’s financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk.
- Processes to identify and ensure compliance with applicable legal and regulatory requirements.

Pexip Responsibility

Pexip’s leadership team is actively committed to the assurance of providing a secure environment that protects and preserves the confidentiality, integrity, authenticity, availability and reliability of information and the service. In regard to a governance framework, Pexip has implemented the ISO/IEC 27001:2013 framework, applying controls from ISO/IEC 27002:2013 as well as numerous controls from NIST SP 800-53r4.

Information security activities are directed by the Chief Information Security Officer (CISO), coordinated by the Security and Compliance Group, and supported by process owners and information asset owners throughout the business.

The company tracks its contractual requirements and regulatory requirements within its ISMS, including regulations such as the GDPR (Regulation EU 2016/679), the Data Protection Act of 2018, and many others.

PRINCIPLE 5: OPERATIONAL SECURITY

NCSC Guidance: The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes. The NCSC guidance points to four elements to consider:

- Configuration and change management – you should ensure that changes to the system have been properly tested and authorised. Changes should not unexpectedly alter security properties
- Vulnerability management – you should identify and mitigate security issues in constituent components
- Protective monitoring – you should put measures in place to detect attacks and unauthorised activity on the service
- Incident management – ensure you can respond to incidents and recover a secure, available service.

These are covered next.

Configuration and Change Management

NCSC Guidance: You should have an accurate picture of the assets which make up the service, along with their configurations and dependencies. Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected. Where change is not effectively managed, security vulnerabilities may be unwittingly introduced to a service. And even where there is awareness of the vulnerability, it may not be fully mitigated.

Goals/Objectives

Ensure the status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime. Ensure changes to the service are assessed for potential security impact. Then managed and tracked through to completion.

Pexip Responsibility

Pexip employs ISO/IEC 27002 controls from A.12.1.2 to ensure changes made are controlled when applicable to the organisation, business processes, information processing facilities and systems that affect information security. In performance of this obligation, Pexip ensures it considers:

- the identification and recording of significant changes;

- planning and testing of changes;
- assessment of the potential impacts, including information security impacts of such changes;
- formal approval procedure for proposed changes;
- verification that information security requirements have been met;
- communication of change details to all relevant persons;
- fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events; and
- provisions of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident.

At Pexip, when changes are made, an audit log containing all relevant information is retained.

Vulnerability Management

Service providers should have a management process in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools. See our guide on vulnerability management for more detail.

Goals/Objectives

The reader should have confidence in Pexip that:

- potential new threats, vulnerabilities or exploitation techniques which could affect the service are assessed and corrective action is taken;
- relevant sources of information relating to threat, vulnerability and exploitation techniques are monitored by the service provider;
- the severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations;
- using a suitable change management process, known vulnerabilities are tracked until mitigations have been deployed; and
- timescales for implementing mitigations are defined and linked to acceptable risk levels.

Pexip Responsibility

Pexip prevents exploitation of technical vulnerabilities by ensuring the organisation's exposure to such is evaluated and appropriate measures taken to address the associated risk. For instance, a complete asset inventory list is maintained including software vendors and hardware deployment. Appropriate

and timely action is taken in response to the identification of potential technical vulnerabilities according to ISO/IEC 27002:2013 guidance from A.12.1.6.

- The organisation has defined and established the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required.
- Information resources are used to identify relevant technical vulnerabilities and to maintain awareness about them. These information resources are updated based on changes in the inventory or when other newer or useful resources are found.
- A timeline has been identified to react to notifications of potentially relevant technical vulnerabilities.
- When technical vulnerabilities are identified, Pexip identifies the associated risks and the actions to be taken; such action may involve patching the vulnerable systems or applying other controls.
- Depending upon the urgency of a technical vulnerability, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures.
- If a patch is available from a legitimate source, the risks associated with installing the patch is assessed, meaning the risks posed by the vulnerability are compared with the risk of installing the patch.
- An audit log is kept for all procedures undertaken.
- Systems at high risk are addressed first.
- An effective technical vulnerability management process is aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur.
- Pexip has defined procedures to address the situation where a vulnerability has been identified but there is no suitable countermeasure. In this situation, the organisation evaluated risks relating to the known vulnerability and defined appropriate detective and corrective actions.

Customer Responsibility

In relation to dedicated platform deployments, customers should stay apprised of Pexip's Security Bulletins

Protective Monitoring

A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of your environments and data.

Goals/Objectives

A good service implementation should:

- ensure the service generates adequate audit events to support effective identification of suspicious activity;
- ensure events are analysed to identify potential compromises or inappropriate use of the service;
- and ensure the service provider takes prompt and appropriate action to address incidents.

Pexip Responsibility

The objective of proper proactive monitoring for Pexip is to record events and generate evidence. Event logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed. Various types of event logs include the following:

- user IDs;
- system activities;
- dates, times and details of key events such as log-on and log-off;
- device identity or location if possible and system identifier;
- records of successful and rejected system access attempts;
- records of successful and rejected data and other resource access attempts;
- changes to system configuration;
- use of privileges;
- use of system utilities and applications;
- files accessed and the kind of access;
- network addresses and protocols;
- alarms raised by the access control system;

- activation and de-activation of protection systems, such as anti-virus system and intrusion detection systems; and
- records of transactions executed by users in applications.

At Pexip, event logging sets the foundation for automated monitoring systems, capable of generating consolidated reports and alerts on system security.

Incident Management

Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users. These processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service.

Goals/Objectives

- Ensure incident management processes are in place for the service and are actively deployed in response to security incidents
- Ensure pre-defined processes are in place for responding to common types of incident and attack
- Ensure a defined process and contact route exists for reporting of security incidents by consumers and external entities
- Ensure security incidents of relevance are reported in acceptable timescales and formats to interested parties

Pexip Responsibility

Incident management at Pexip ensures a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. The following processes are practices in accordance with ISO/IEC 27002:2013 A.16.

- Incident management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents. These include:
  - Procedures for incident response planning and preparation;
  - Procedures for monitoring, detecting, analysing and reporting of information security events and incidents;
  - Procedures for logging incident management activities;
  - Procedures for handling of forensic evidence;

- Procedures for assessment of and decision on information security events and assessment of information security weaknesses;
- Procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organisations.

- Incident management procedures are established to ensure competent handling of issues related to information security incidents within the organisation, along with a point of contact for security incident detection and reporting, and appropriate contact with authorities, external interest groups or forms that handle the issues related to information security incidents.
- The reporting of information security events are reported through appropriate channels as quickly as possible.
- The reporting of information security weaknesses is supported by an internal portal along with an automated monitoring system.
- Assessment of and decision on security events is handled by appropriate personnel, classified when appropriate as an information security event.
- Response to information security incidents is taken in accordance with ISMS documented procedures. When appropriate, evidence is collected as soon as possible after the occurrence. A forensic analysis is conducted when appropriate. All involved response activities are logged for later analysis.
- Learning from information security incidents is practiced, aiming for knowledge to be gained from analysing and resolving information security incidents to reduce the likelihood or impact of future incidents.
- The collection of evidence ensures identification, collection, acquisition and preservation of information which can serve as evidence.

PRINCIPLE 6: PERSONNEL SECURITY

NCSC Guidance: Where service provider personnel have access to customer data and systems a high degree of confidence is needed in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

The service provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles.

Goals/Objectives

A good service implementation should:

- Ensure the level of security screening conducted on service provider staff with access to customer information, or with ability to affect the service, is appropriate.
- Ensure the minimum number of people required have access to customer information or could affect the service.

Pexip Responsibility

Pexip ensures that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered and employed. Toward this, Pexip employs three practices concomitant to human resource security: prior to employment practices, during employment practices, and post-employment practices. These will be extrapolated here.

Prior to Employment

Before hiring any candidate, Pexip employs verification checks on all candidates in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. Where possible, Pexip checks:

- availability of satisfactory character references, e.g. one business and one personal;
- a verification (for completeness and accuracy) of the applicant's curriculum vitae;
- confirmation of claimed academic and professional qualifications;
- independent identity verification (passport or similar document); and
- more detailed verification, such as credit review or review of criminal records.

During Employment

Pexip requires all its employees and contractors to apply information security in accordance with the established policies and procedures of the organisation. Toward this, management ensures all employees and contractors:

- are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems;

- are provided with guidelines to state information security expectations of their role within the organisation;
- are motivated to fulfil the information security policies of the organisation;
- achieve a level of awareness on information security relevant to their roles and responsibilities within the organisation;
- conform to the terms and conditions of employment, which includes the organisation's information security policy and appropriate methods of working;
- continue to have the appropriate skills and qualifications and are educated on a regular basis; and
- are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Post-Employment

To protect the organisation's interests as part of the process of changing or terminating employment, Pexip maintains termination or change employment processes and procedures. Access privileges are suspended when applicable, and changes of employment are communicated to workforce in writing. Third parties may be notified when appropriate.

PRINCIPLE 7: SECURE DEVELOPMENT

NCSC Guidance: Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

Goals/Objectives

- Ensure new and evolving threats are reviewed and the service improved in line with them.
- Ensure development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.
- Ensure configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.

Pexip Responsibility

Pexip maintains policies to ensure information security is designed and implemented within the development lifecycle of the Pexip service. Rules have been established that comply with OWASP

Security Design Principles. Secure development at Pexip is a requirement; it permeates services, architecture, software and systems. The secure development policy takes into consideration the following:

- security of the development environment;
- guidance on the security in the software development lifecycle for (a) security in the software development methodology, and (b) secure coding guidelines for each programming language used.
- security requirements in the design phase;
- security checkpoints within the project milestones;
- secure repositories;

  security in the version control;
- required application security knowledge; and
- developers' capability of avoiding, finding and fixing vulnerabilities.

These security techniques are employed for both new developments as well as code reuse scenarios. In following these practices, Pexip complies with the guidelines established in ISO/IEC 27002:2012 A.14.2.1.

PRINCIPLE 8: SUPPLY CHAIN SECURITY

NCSC Guidance: The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

Cloud services often rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Goals/Objectives

- Transparently communicate how information is shared with, or accessible to, third party suppliers and their supply chains.
- Ensure procurement processes place security requirements on third party suppliers.
- Ensure security risks from third party suppliers are managed.

- Ensure suppliers conform with security requirements.
- Ensure hardware and software used in the service is genuine and has not been tampered with.

Pexip Responsibility

Pexip ensures protection of the organisation's assets and the customer's data when accessed by suppliers. All suppliers are vetted according to the policy in ISO/IEC 27002:2013 A.15 for establishing secure supplier relationships. When determining supplier assurances, Pexip:

- addresses security within supplier agreements, ensuring flowdown terms from contractual requirements and data privacy laws are upheld;
- ensures agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain;
- and monitors and review supplier services, auditing supplier service delivery and SLA adherence;
- manages changes to supplier services, including the provision of services by suppliers by maintaining and improving existing information security policies, procedures and controls, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

Critical to the service delivery of the Pexip service, several suppliers in the form of subprocessors (per GDPR parlance) are employed. These suppliers are vetted according to the criteria listed above. A list of the current subprocessors employed may be found here.

Customer Responsibility

In relation to customers desiring calendar integration, customer dedicated platform deployments are utilized for both the service and customer dedicated platforms. More information may be found here.

PRINCIPLE 9: SECURE USER MANAGEMENT

NCSC Guidance: Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

The aspects to consider are:

- Authentication of users to management interfaces and support channels

- Separation and access control within management interfaces

Each of these practice areas are described below.

Authentication of Users to Management Interfaces and Support Channels

NCSC Guidance: In order to maintain a secure service, users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service.

These activities may be conducted through a service management web portal, or through other channels, such as telephone or email. They are likely to include such functions as provisioning new service elements, managing user accounts and managing consumer data.

Service providers need to ensure that all management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data. Service providers need to ensure that all management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data.

Goals/Objectives

You should have sufficient confidence that:

- You are aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone phone, web portal, email etc.).
- Only authorised individuals from your organisation can use those mechanisms to affect your use of the service. (Principle 10 can help you consider the strength of user identification and authentication in each of these mechanisms.)

Pexip Responsibility

Pexip maintains a partner portal supporting identity and access management services to provide mechanisms that ensure only permissioned resources may access user configuration, privileges and records. The partner portal permits administrative actions to be performed to provision users, set credentials, reset credentials, suspend or terminate users, check logging activity, troubleshoot call setup and support, and numerous other features.

Separation and Access Control Within Management Interfaces

NCSC Guidance: Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If users are not adequately separated within management interfaces, one user may be able to affect the service, or modify the data of another.

Your privileged administrative accounts probably have access to large volumes of data. Constraining the permissions of individual users to those absolutely necessary can help to limit the damage caused by malicious users, compromised credentials or compromised devices.

Role-based access control provides a mechanism to achieve this and is likely to be a particularly important capability for users managing larger deployments.

Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to one of these networks. Guidance on assessing the risks of exposing interfaces to different types of networks is provided under Principle 11.

Goals/Objectives

A good service implementation should:

- have confidence that other users cannot access, modify or otherwise affect your service management
- manage the risks of privileged access using a system such as the 'principle of least privilege'
- understand how management interfaces are protected (see Principle 11) and what functionality they expose.

Pexip Responsibility

Access controls within management interfaces follow the guidelines of ISO/IEC 27002:2013 controls A.9, limiting access to information and Information processing facilities. This consists of an access control policy that takes into consideration the following:

- security requirements of business applications in regard to management interfaces;
- policies for information dissemination and authorization (i.e., the need to know principle and information security levels and classifications);
- consistency between access rights and information classification policies;
- relevant legislation and any contractual obligation regarding limitation of access to data;

- management of access rights in distributed networked environments;
- segregation of access control roles;
- requirements for formal authorization of access requests;
- requirement for periodic review of access rights;
- removal of access rights;
- archiving of records of all significant events concerning the use and management of user identifies and secret authentication information;
- roles with privileged access.

Access to networks and network services is only provided with access to the network and network services that have been specifically authorized.

Note: In relation to dedicated platform deployments, administrative access is backed by the customer's Active Directory LDAP backend with role-based access control centred on AD groups. For more information refer to: https://docs.pexip.com/admin/managing_users.htm

PRINCIPLE 10 IDENTITY AND AUTHENTICATION

NCSC Guidance: All access to service interfaces should be constrained to authenticated and authorised individuals. Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service. Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks.

Goals/Objectives

A good service implementation should provide confidence that identity and authentication controls ensure users are authorised to access specific interfaces.

Pexip Responsibility

Identity, authentication and access management (IAM) is a core tenet of the Pexip cloud service, and Pexip employs various ways to identify valid subscribers and administrators of the platform, including provisioned users or Active Directory integration with single sign-on. For instance, in large organisations with many employees and users of video conferencing, an organisation may need to configure many Virtual Meeting Rooms (VMRs) and associated records to support those employees.

The Pexip support organization can work with customers who want to bulk provision accounts which will leverage Active Directory for SSO access. Alternatively, Pexip's service portal is accessible to account administrators via traditional sign-on methods provisioned by an account administrator. The service portal does not enforce two factor authentication, however it is subject to Pexip's password policy.

Pexip's analytics portal is only available via two factor authentication.

Note: In relation to dedicated platform deployments, customers may choose to protect client and admin interfaces with multiple levels of authentication, including custom solutions for conference join requests (i.e. for integrations with EHR / patient data systems or similar) by utlizing External Policy. For more information please refer to: https://docs.pexip.com/admin/using_policy.htm

PRINCIPLE 11: EXTERNAL INTERFACE PROTECTION

NCSC Guidance: All external or less trusted interfaces of the service should be identified and appropriately defended.

If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant. You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk.

Goals/Objectives

A good service implementation should:

- Articulate the physical and logical interfaces information is available from, and how access to service data is controlled.
- Instil confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10).

Pexip Responsibility

Pexip uses a customized, cut-down version of Linux which has been designed to avoid exposing unnecessary network services and thus naturally limits the "attack surface" available to an attacker. Pexip regularly releases new software versions which incorporate the very latest operating system security patches (see Pexip security bulletins for more information).

All public access points into the Pexip Service are protected by firewall and IDS to prevent unauthorized access. User authentication can be integrated with identity management systems via SAML 2.0 (including directly with Active Directory) or Google identity authentication, whichever the customer would prefer.

PRINCIPLE 12: SECURE SERVICE ADMINISTRATION

*NCSC Guidance: S*ystems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data. The design, implementation and management of administration systems should follow enterprise good practice, whilst recognising their high value to attackers.

Goals/Objectives

A good service implementation should:

- Articulate which service administration model is being used by the service provider to manage the service.
- Convey the risks the service administration model in use brings to service data or use of the service.

Pexip Responsibility

The NCSC explains five administrative models for secure service administration:

- dedicated devices on a segregated network;
- dedicated devices for community service administration;
- dedicated devices for multiple community service administration;
- service administration via bastion hosts; and
- direct service administration.

Pexip meets the criteria of “dedicated devices for multiple community service administration”. Access to the administrative interface operates on a least permissions model. When a user logs into the admin portal, they can only see their organization or any organization listed as children under their parent organization; they are not permitted to see any parent organization or other child organizations of their parent.

PRINCIPLE 13: AUDIT INFORMATION FOR USERS

NCSC Guidance: You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

Goals/Objectives

A good service implementation should:

- Clarify the audit information that will be provided to customers, how and when it will be made available, the format of the data, and the retention period associated with it.
- Ensure audit information available meets the needs for investigating misuse or incidents

Pexip Responsibility

Logging facilities and logging information is protected against unauthorized access and tampering. Logging includes access controls and call detail records, enabling tabulation of usage statistics that go back three months. The clocks of all relevant information processing systems within the Pexip cloud security domain are synchronised to a single reference time source using the network time protocol. This ensures the accuracy of audit logs, which may be required for investigation or as evidence in legal cases.

Note: In relation to dedicated platform deployments, administrators may set up syslog to externalize storage of all events if desired for externalized storage of audit trails.

PRINCIPLE 14: SECURE USE OF THE SERVICE

NCSC Guidance: The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

The extent of your responsibility will vary depending on the deployment models of the cloud service, and the scenario in which you intend to use the service. Specific features of individual services may

also have bearing. For example, how a content delivery network protects your private key, or how a cloud payment provider detects fraudulent transactions, are important security considerations over and above the general considerations covered by the cloud security principles.

With IaaS and PaaS offerings, you are responsible for significant aspects of the security of your data and workloads. For example, if you procure an IaaS compute instance, you will normally be responsible for installing a modern operating system, configuring that operating system securely, securely deploying any applications and also maintaining that instance through applying patches or performing maintenance required.

Goals/Objectives

A good service implementation should:

- Clarify service configuration options available to users and the security implications of the configuration option(s)
- Convey the security requirements of the use of the service
- Publish user guides and/or training materials to ensure customers are educated on using and managing the service safely and securely.

Pexip Responsibility

Pexip maintains a publicly accessible repository of end user support materials for the service and its applications. The configuration options that are available to administrators and users are described and general information on using and troubleshooting the service are available. Topics that are covered include:

- Company usage statistics for Administrators
- Pexip SSO Provider and Entity Information
- List of protocols, codecs and resolutions supported in the Pexip Service
- Firewall Rules and Domain Hosting
- Recommended Bandwidth at Office Location
- PC Specification & Network Requirements
- Downloading the Pexip app and Logging In
- Receiving and Making Calls with Video Addresses Outside Your Company Network
- Using My Meeting Video clients in a remote desktop environment

- Group Policy Blocking; Locking a room
- VMR PIN brute force attack resistance
- Pexip app Guest Users
- Chat during meetings
- General information on content sharing in VMRs
- Virtual Meeting Room dial-in information
- How do PINs on VMRs work
- How does the VMR layout work
- Disconnect policies on VMRs, to name a few.

Customer Responsibility

It is the customers responsibility to train and educate its users on how to use and administer the services subscribed to.

It is the customers responsibility to secure their endpoints (applications and devices) that access the service. Unsecured endpoints are susceptible to attack and misuse.

Note: In relation to dedicated platform deployments, administrators can choose to enforce encryption globally. For more information, please refer to: https://docs.pexip.com/admin/global_settings.htm#encryption) or pr meeting service. Services deemed not required, or not preferred to be enabled (I.e. H323) can be disabled

CONCLUSION

Ongoing research indicates that data breaches are on the rise at a time when cloud services are failing to protect organisational information. It is more important than ever to vet suppliers and ensure they implement compliance safeguards using technical, administrative, physical and legal controls to secure the confidentiality, integrity and availability of customer information.

Pexip has written this whitepaper in a transparent manner to convey the practices it employs in the context of the NCSC's 14 Cloud Security Principles. If there are additional questions your organisation wants to ask, please write to this email address and Pexip will respond to your inquiry in a timely manner:

privacy@pexip.com

If your organisation would like to have a discussion regarding security and data privacy compliance practices, Pexip is happy to meet and support that discussion.

Additional resources are noted here that may be of interest.

https://www.pexip.com/security

ANNEX A: DESCRIPTION OF PERSONAL DATA PROCESSED

Personal data that will be processed in the scope of the Service Agreement and the purposes for which these data will be processed are defined as follows:

Subject Matter

The subject matter of this Addendum relates to the Data Processor's services, including voice, video, chat, content sharing and file distribution, which is also supported by the Infinity platform, including service desk support.

Purpose of Processing

The Data Processor processes Personal Data on behalf of the Data Controller in order to provision and provide services to the Data Controller. According to the Service Agreement, the subject matter, purpose of data processing, nature of data processing, and categories of data subjects are defined below.

Nature of Data Processing

Personal data may be collected according to the Services Agreement to support the service, and the processing activity may involve collection, storage, duplication, electronic viewing, deletion and destruction of personal data.

Categories of Data Subjects

The categories of data subjects may include employees of the Data Controller or End Customer and its affiliates, including partners and contractors and, the Data Controller's or End Customer's meeting participants.

Provisioning Data

The following provisioning data is collected to establish services for video users. This information is stored and associated with an individual's profile.

- Contact Name
- Email Address
- Dialling Address

Meeting Metadata

The following information is collected only if a person uses the portal to schedule a meeting and invite other participants.

- Meeting Title
- Meeting participant names
- Call log details
  - Display name of participants
  - Inbound URIs and/or IP addresses of participants
  - Inbound telephone numbers
  - Call duration

Conference Media

The following media may be processed during any video conferencing session:

- Audio streams
- Video streams
- Content sharing

Chat Messages

The following information may be collected if a person uses the chat tool to relay instant messages to others or groups attending the meeting.

- Participant Name
- Chat Message
- Timestamp of Message
- Files transferred (when applicable)

Reporting Data

The following information is stored in a database to facilitate generating a report for the purpose of support and audit, and to provide utilization metrics in regard to the service.

- Meeting Title
- Meeting Participant Names

- Call Log Details
  - Display Name of Participants
  - Inbound URIs and/or IP Addresses of Participants
  - Call Duration

Support Data

The following data could be associated with incident management (ticketing), if a user opens a ticket with the support desk and requests help to redress a conference issue.

- Contact Name
- Email Address
- Phone Number
- Call/Meeting Data
- Device logs: Call log details if applicable for troubleshooting, which usually includes H323 and SIP call negotiation and maintenance events from the local and remote terminals.

Device specific details such as applications, operating system, hardware components, performance metrics, and firmware, application names for applications that are able to be shared from the end user's device, global contact/address lists associated with the device.