Zoom Video Communications
Cloud Security Principles

20th May 2020

Approved for Public Release
Introduction ........................................................................................................................................... 5

Document Format .................................................................................................................................... 5

1. NCSC Cloud Security Principle: Data in transit protection ............................................................... 5
   Goals ....................................................................................................................................................... 5
   Zoom responsibility ............................................................................................................................... 5
   Customer responsibility ......................................................................................................................... 6

2. NCSC Cloud Security Principle: Asset protection and resilience ..................................................... 7
   2.1. NCSC Consideration: Physical location and legal jurisdiction ..................................................... 7
       Goals ..................................................................................................................................................... 7
       Zoom responsibility ............................................................................................................................ 7
       Customer responsibility ..................................................................................................................... 8
   2.2. NCSC Consideration: Data centre security .................................................................................. 8
       Goals ..................................................................................................................................................... 8
       Zoom responsibility ............................................................................................................................ 8
   2.3. NCSC Consideration: Data at rest protection .............................................................................. 8
       Goals ..................................................................................................................................................... 9
       Zoom responsibility ............................................................................................................................ 9
   2.4. NCSC Consideration: Data sanitisation ...................................................................................... 10
       Goals .................................................................................................................................................... 10
       Zoom responsibility ............................................................................................................................ 10
       Customer responsibility ................................................................................................................... 10
   2.5. NCSC Consideration: Equipment disposal ................................................................................. 10
       Goals .................................................................................................................................................... 10
       Zoom responsibility ............................................................................................................................ 11
   2.6. NCSC Consideration: Physical resilience and availability ............................................................ 11
       Goals .................................................................................................................................................... 11
       Zoom responsibility ............................................................................................................................ 11

3. NCSC Cloud Security Principle: Separation between users ............................................................ 12
   Goals ...................................................................................................................................................... 12
   Zoom responsibility .............................................................................................................................. 13
   Customer responsibility ....................................................................................................................... 13
4. NCSC Cloud Security Principle: Governance framework .............................................. 13
   Goals.......................................................................................................................... 13
   Zoom responsibility........................................................................................................ 14
5. NCSC Cloud Security Principle: Operational security ...................................................... 14
   5.1. NCSC Consideration: Configuration and change management .................................. 15
       Goals.......................................................................................................................... 15
       Zoom responsibility.................................................................................................... 15
       Customer responsibility .............................................................................................. 15
   5.2. NCSC Consideration: Vulnerability management ...................................................... 16
       Goals.......................................................................................................................... 16
       Zoom responsibility.................................................................................................... 16
   5.3. NCSC Consideration: Protective monitoring .............................................................. 17
       Goals.......................................................................................................................... 17
       Zoom responsibility.................................................................................................... 17
       Customer responsibility .............................................................................................. 18
   5.4. NCSC Consideration: Incident management .............................................................. 18
       Goals.......................................................................................................................... 18
       Zoom responsibility.................................................................................................... 18
       Customer responsibility .............................................................................................. 19
6. NCSC Cloud Security Principle: Personnel security ......................................................... 19
   Goals.......................................................................................................................... 19
   Zoom responsibility........................................................................................................ 19
7. NCSC Cloud Security Principle: Secure development ........................................................ 20
   Goals.......................................................................................................................... 20
   Zoom responsibility........................................................................................................ 20
8. NCSC Cloud Security Principle: Supply chain security ...................................................... 21
   Goals.......................................................................................................................... 21
   Zoom responsibility........................................................................................................ 21
9. NCSC Cloud Security Principle: Secure user management ................................................ 22
   9.1. NCSC Consideration: Authentication of users to management interfaces and support 
       channels ..................................................................................................................... 22
       Goals.......................................................................................................................... 23
9.2. NCSC Consideration: Separation and access control within management interfaces ........................................... 24
   Zoom responsibility .................................................................................................................................................... 25
   Customer responsibility ............................................................................................................................................... 25

10. NCSC Cloud Security Principle: Identity and authentication ................................................................. 25
    Goals ........................................................................................................................................................................ 25
    Zoom responsibility .................................................................................................................................................... 25
    Customer responsibility ............................................................................................................................................... 26

11. NCSC Cloud Security Principle: External interface protection ........................................................... 26
    Goals ........................................................................................................................................................................ 26
    Zoom responsibility .................................................................................................................................................... 26
    Customer responsibility ............................................................................................................................................... 26

12. NCSC Cloud Security Principle: Secure service administration ............................................................ 27
    Goals ........................................................................................................................................................................ 27
    Zoom responsibility .................................................................................................................................................... 27
    Customer responsibility ............................................................................................................................................... 27

13. NCSC Cloud Security Principle: Audit information for users .......................................................................... 28
    Goals ........................................................................................................................................................................ 28
    Zoom responsibility .................................................................................................................................................... 29
    Customer responsibility ............................................................................................................................................... 29

14. NCSC Cloud Security Principle: Secure use of the service ................................................................. 29
    Goals ........................................................................................................................................................................ 29
    Zoom responsibility .................................................................................................................................................... 30
    Customer responsibility ............................................................................................................................................... 30
Introduction
Zoom is the leader in modern enterprise video communications, with an easy, reliable cloud platform for video and audio conferencing, collaboration, chat, and webinars across mobile devices, desktops, telephones, and room systems. Zoom Rooms is the original software-based conference room solution used around the world in board, conference, huddle, and training rooms, as well as executive offices and classrooms. Founded in 2011, Zoom helps businesses and organizations bring their teams together in a frictionless environment to get more done. Zoom is a publicly traded company on Nasdaq (ticker: ZM) and headquartered in San Jose, California.

Document Format
Each NCSC Cloud Security Principle is represented by a heading. Some Cloud Security Principles also contain NCSC Considerations, which are also represented by subheadings. All principles and considerations are followed by NCSC Guidance and goals, which are formatted in italics. Please note that all principles, considerations and guidance are taken from NCSC’s documentation and are not written by Zoom.

Zoom’s responses to NCSC’s principles, considerations and guidance can be found under the subheadings Zoom responsibility and where appropriate, any customer responsibility.

1. NCSC Cloud Security Principle: Data in transit protection
   NCSC Guidance: User data transiting networks should be adequately protected against tampering and eavesdropping.
   This should be achieved through a combination of:
   - network protection - denying your attacker the ability to intercept data
   - encryption - denying your attacker the ability to read data

Goals
You should be sufficiently confident that:
   - Data in transit is protected between your end user device(s) and the service
   - Data in transit is protected internally within the service
   - Data in transit is protected between the service and other services (e.g. where APIs are exposed)

Zoom responsibility
Zoom Meetings and Webinars – This includes all audio, video and shared content. Zoom encrypts in-meeting and in-webinar content between each end users device via the cloud service (data is not de-encrypted when it is in the Zoom cloud service (The Facts Around Zoom and Encryption for Meetings/Webinars) using TLS 1.2 or higher for signalling and exchanging encryption keys, and
Advanced Encryption Standard (AES) using a 256 bit key for the media (audio, video and shared content).

**Data in transit** is also protected between services when using the Zoom API’s with TLS 1.2, also the Zoom API’s are using OAuth (Client ID and Client Secret) and JWT (API Key & Secret) to authenticate the API requests.

H.323/SIP Devices: H.323 or SIP devices joining a Zoom meeting connect to Zoom’s Cloud Room Connector using the industry standard, Advanced Encryption Standard (AES) 128-bit algorithm. Cloud Room Connector follows the process listed above. The key used for the desktop and mobile clients may be different than the key used for H.323 or SIP devices. Encryption must also be enabled on the device. If the encryption setting is enabled and AES-128 encryption is not available or is turned off on the H.323 or SIP device, it will be unable to join the meeting and will receive an error message about enabling encryption for the device.

For dial-in participants, as the call transitions from the PSTN network to the Zoom cloud, the Zoom telephony gateway servers encode and encrypt the audio following the standard client process outlined above. However, encryption across the PSTN itself is not possible.

For chat (instant messaging), end-to-end chat allows for a secured communication where only the intended recipient(s) can read the secured message. Zoom uses a combination of asymmetric (public-private key) and symmetric (shared session key) encryption to protect the chat sessions. Zoom uses device level authentication to ensure messages can only be ready by the intended recipient on an authorized device.

Symmetric keys use to encrypt meeting related data are only stored in memory (server and client) and are purged once the meeting and any meeting related customer requests are completed.

A detailed description of Zoom's encryption can be found in our [Encryption Whitepaper](#). Please also review the [security whitepaper](#). Zoom also complies with the [TLS standards](#) set out by the NCSC.

**Customer responsibility**

Encryption can be required for H.323 and SIP devices joining Zoom meetings. This setting is configured at the account level, group, or user level. Once enabled, encryption will need to be enabled on these devices when joining your Zoom meeting or they will receive an error and be unable to join.

Zoom allows customers to select the regions used for data routing from the administration settings, this can be adjusted at account, group or user level and allows data in transit to be enabled or disabled in the following regions:

- Australia
- Canada
- China
- Europe
- Hong Kong
- India
- Japan
2. NCSC Cloud Security Principle: 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 aspects to consider are:

- Physical location and legal jurisdiction
- Data centre security
- Data at rest protection
- Data sanitisation
- Equipment disposal
- Physical resilience and availability

2.1. NCSC Consideration: Physical location and legal jurisdiction

**NCSC Guidance:** In order to understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed.

You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation. Inappropriate protection of user data could result in legal and regulatory sanction, or reputational damage.

**Goals**

You 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 e.g. Data Protection Act (DPA)
- Whether the legal jurisdiction(s) within which the service provider operates are acceptable to you

**Zoom responsibility**

As a global service provider, Zoom processes data globally in order to provide the service. By default, customer data is persistently stored in AWS in the United States; however, there are exceptions for customers located in the EU and Canada. If a customer account is created within the EU region then their data can be migrated to the AWS cluster in the EU (Frankfurt and Dublin).

Customer agreements are concluded with Zoom Video Communications, Inc. That notwithstanding, Zoom is able to amend the governing law of any subscription to reflect that of England and Wales. All subscription agreements are drafted in accordance with applicable laws, and are complemented by our data processing agreement which is, among others, GDPR compliant.

Zoom stores its data at rest in AWS, but some data (cloud recordings and meta data, is stored at the co-locations temporarily before it is moved to AWS) may be hosted in its co-located datacentres worldwide.
that are used to facilitate real-time meeting services. Meeting participants are connected to the co-location nearest to their geographic location. Cloud recordings are temporarily stored in the co-locations for up to 30 days before being sent to Zoom’s AWS instance for permanent storage. Meeting logs are removed from the co-locations and sent to Zoom's AWS instance on a daily basis.

Further details are available on Zoom’s privacy policy.

**Customer responsibility**
If you require data to be stored within the EU, you will need to make this request to Zoom.

### 2.2. NCSC Consideration: 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**
*You should be confident that the physical security measures employed by the provider are sufficient for your intended use of the service.*

**Zoom responsibility**
Zoom has a formal Physical and Environmental policy in place. Physical access to Zoom's office facilities is protected by 24x7 camera surveillance, keycode/RFID access, and staffed reception. Additionally, Zoom leverages the physical and environmental protection of its Tier 3 and above datacentre providers. Only authorized personnel have access to Zoom's datacentres.

In the datacentres, physical access is controlled by access list, badge, mantrap, guards, perimeter fencing, CCTV, and biometrics. All visitors must be escorted by authorized Zoom personnel at all times. The datacentres uphold the necessary safety requirements for fire protection and utilize solid building construction to safeguard assets.

Zoom undergoes an annual SOC 2 Type II assessment. The 2019 SOC 2 report can be shared under a signed NDA.

For the AWS environment, Zoom leverages [AWS physical security safeguards](https://aws.amazon.com/security/). You can also view the [AWS 14 Cloud Security Principles](https://docs.aws.amazon.com/security/latest/securityguide/).

### 2.3. NCSC Consideration: Data at rest protection

**NCSC Guidance:** To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be 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
*You should have sufficient confidence that storage media containing your data are protected from unauthorised access.*

Zoom responsibility
Customer data is stored in AWS. Cloud recordings are only temporarily stored in the co-locations before being sent, over an encrypted TLS 1.2 link, to Zoom’s AWS instance for permanent storage. Meeting logs are removed from the co-locations and sent to Zoom’s AWS instance on a daily basis.

Data elements stored and/or processed by Zoom platform are as follows:

- Customer Account Information: Company Name, Customer Account Owner Contact Information (Name, Email, Phone), Customer Business Contact Information (Name, Email, Phone), Business Address, Customer Account Type, Customer Account Plan, Scheduled Meetings
- User Profile: First Name, Last Name, Phone (optional), Email, Password (if SSO is not used), Profile Picture (optional), Department (optional)
- Meeting Metadata: Topic, Description (Optional), Participant IP Addresses, Device/Hardware Information, Meeting Statistics/Metrics, Start Time, Join Time, Leave Time
- Some additional option data elements include IM chat logs and metadata and cloud meeting recordings.

Data at rest and storage used by compute (EC2) is protected leveraging Amazon Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256) in Amazon S3, Amazon DynamoDB, or Amazon RDS. Zoom leverages AWS KMS. Encryption keys are managed by AWS Key Management Services (KMS). AWS KMS keys are not visible to Zoom and are completely managed by AWS.

AWS KMS is designed so that no one, including AWS employees, can retrieve the plaintext master keys from the service. The service uses hardware security modules (HSMs) that have been validated under FIPS 140-2, or are in the process of being validated, to protect the confidentiality and integrity of the keys regardless of whether we are use AWS KMS or AWS CloudHSM to create your keys or you import them into the service. Plaintext keys never leave the HSMs, are never written to disk and are only ever used in the volatile memory of the HSMs for the time needed to perform the requested cryptographic operation. AWS KMS keys are never transmitted outside of the AWS regions in which they were created. Updates to software on the service hosts and to the AWS KMS HSM firmware is controlled by multi-party access control that is audited and reviewed by an independent group within Amazon as well as a NIST-certified lab in compliance with FIPS 140-2.

Zoom performs continuous incremental backups and daily snapshots of the production databases on Amazon AWS. Backup files are securely transferred to AWS for storage. Data stored in Amazon S3, Amazon DynamoDB, or Amazon RDS is redundantly stored in multiple physical locations as part of normal operation of those services. Zoom has reviewed the AWS SOC-2 Report and has determined the AWS backup systems meet company requirements. AWS KMS whitepaper
2.4. NCSC Consideration: 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
  - your data being lost or disclosed on discarded, lost or stolen media

**Goals**

*You should be sufficiently confident that:*

- Your data is erased when resources are moved or re-provisioned, when they leave the service or when you request it to be erased
- Storage media which has held your data is sanitised or securely destroyed at the end of its life

**Zoom responsibility**

Data at rest is protected leveraging Amazon Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256). Customer content is retained for the life of the account; however, customers are free to delete this content at any time. When an account is terminated, customer content is deleted after 60 days or as agreed in a separate contract. Account information is information provided to Zoom when a user or company signs up for the Service. Customer content is information provided by the customer to Zoom through the usage of the service. Customer content includes cloud recordings and instant messages.

Zoom does not allow portal media devices to the production environment, all data stored in the colocations and AWS is securely destroyed at the end of its lifecycle.

**Customer responsibility**

Customers can set custom retention periods and delete data as a self-service via in-product features and tools.

2.5. NCSC Consideration: 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**

*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.
Zoom responsibility
Zoom has a documented Asset Disposal Policy and an Asset Management Policy in place, these are available under NDA. For corporate and production assets, certificates of destruction/disposal are provided by the third-party handling the asset destruction/disposal. Additionally, Zoom leverages third-party shredding services for document disposal in Zoom offices.

Zoom has reviewed the AWS SOC 2 report and determined that AWS's controls related to asset management are sufficient. Zoom performs annual due diligence on AWS and all other critical vendors.

2.6. NCSC Consideration: 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 your business.

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

Zoom responsibility
Zoom systems are designed and engineered with the goal of minimizing or eliminating critical points of failure. Zoom has 2 types of data centres, co-located datacentres for meeting traffic and AWS clusters to store data that has resulted from the meetings.

For the meeting stream, resilience is achieved through the ability for the meeting data centres to share load between each other. These data centres, co-located at vendor facilities, are maintained to have capacity of double the previous peak volume to give sufficient headroom for growth.

For the meeting data, Zoom relies on AWS resilience within regional clusters as described by AWS documentation. For example, in Europe, If the Dublin instance was unavailable then the service would remain available from the Frankfurt AWS instance (ensuring that your data remains in region).

Zoom has a Business Continuity / Disaster Recovery Plan in place. (Available under NDA).

Zoom conducts annual testing and review fail-over of its Disaster Recovery (DR) Plan. Zoom’s DR plan is activated in the event of a total facility failure due to fire or other natural or man-made disaster. Zoom maintains redundant/highly available datacentres across the globe, including two in the EU. Services have been designed to withstand full datacentre outages.

Our approach means that no single component failure should disable the entire system or even large parts of the system for any appreciable amount of time. Even the unlikely event of simultaneous multiple component failures should not disable a large portion of Zoom’s systems. The following items illustrate Zoom’s components that support a high-availability system:

- Redundant facilities
- Telephony infrastructure
• Internet service, LAN connection, security and related infrastructure
• Relational database management system
• Mass storage systems
• Backups
• Hardware / infrastructure
• System capacity
• Capacity management
• Maintenance / failure allowance

Zoom's co-located facilities are N+1 and have environmental controls such as:

• Temperature and Humidity Controls
• Power systems that are fully redundant and scaled to accommodate component failure.
• Has resilient emergency lighting in place
• Emergency Lighting
• Fire Protection
• Water Damage Protection

SLAs are addressed in Zoom’s Master Services Agreement (MSA) and may include 99.9% uptime, excluding excused downtime (maintenance). Zoom shall make commercially reasonable efforts to ensure that Downtime does not exceed 0.1% in a month. In the event of any Downtime of the Services in excess of 0.1% in a month, Zoom shall provide Customer a credit in an amount equal to the Downtime percentage times Customer’s monthly subscription amount for the Service. Customer shall provide Zoom with prompt written notice of any Downtime. If Zoom fails to correct any Downtime situation within fifteen (15) business days after receipt of such notice, Customer may terminate this Agreement.

3. NCSC Cloud Security Principle: 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.

Factors affecting user separation include:

- where the separation controls are implemented – 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)
- the level of assurance available in the implementation of separation controls

**Goals**

You:

- understand the types of user you share the service or platform with
- have confidence that the service provides sufficient separation of your data and service from other users of the service
- have confidence that management of your service is kept separate from other users (covered separately as part of Principle 9)

Zoom responsibility
As with all software as a service, Zoom operates a multi-tenanted hosted application, meaning that the multiple clients of Zoom share application infrastructure and customer specific encryption is applied to all data to guarantee separation.

Customer data is also logically segregated.
- Each customer will have a unique URL.
- Each customer has a unique ID, called Account ID. Like UXAX-XXXX-XXXX. Customer DB records is associated with this account ID.
- Customer storage top folder name uses Account ID.

This is standard for cloud solution providers.

Customer responsibility

Best Practises for Securing Your Zoom Meetings

4. NCSC Cloud Security Principle: 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
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.
Zoom responsibility

Zoom's information security programs are led by Zoom's Chief Information Security Officer (CISO) and the Head of Product Security. Zoom has corresponding dedicated security teams for both Zoom Product Security and Zoom Corporate Security.

Zoom follows the recommended security controls established by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Included in our security framework (Zoom have completed the self-assessment with the CSA) are role-based security access controls (RBAC) that enable or prevent access to client data based on the principle of "least privilege" necessary for an employee’s job function. Additionally, technologies are in place to protect against outside threats, including controls such as network perimeter firewalls, security groups, intrusion detection systems, security information and event management (SIEM), endpoint anti-malware protections, and company-wide multi-factor authentication to Zoom IT resources.

Zoom's Risk Assessment Policy requires Zoom to carry out comprehensive infrastructure analyses and to employ risk assessment strategies in order to effectively determine, assess and document relevant risks.

Zoom is able to amend the governing law of any subscription to reflect that of England and Wales. Visit our [Legal & Privacy](#) site for more information.

Zoom complies with the following:

- [EU-US and Swiss-US Privacy Shield](#)
- FedRAMP: Zoom for Government is [FedRAMP Authorized](#) (impact level: Moderate)
- [GDPR Compliance](#)
- [HIPAA Business Associate Agreement](#)
- PCI DSS: Zoom leverages PCI-DSS compliance by self-assessing PCI DSS compliance through [Trustwave](#)
- SOC 2 Type II
- SOX: As of Q1 FY20, Zoom conducts quarterly Section 302 and Section 906 certifications, which will be included with the 10Q SEC file. Additionally, a Section 404A certification will be conducted annually and will be included with the 10K file.

5. NCSC Cloud Security Principle: 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.

There are 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
5.1. NCSC Consideration: 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**

You should have confidence that:

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

**Zoom responsibility**

Zoom's asset management tool tracks the following information for production assets: host name, IP addresses, OS, geographical region, datacentre location, rack location, application type, environment such as prod/dev/stage, serial number, and switch port. Zoom has a documented Asset Disposal Policy and an Asset Management Policy in place. For corporate and production assets, certificates of destruction/disposal are provided by the third-party handling the asset destruction/disposal. Additionally, Zoom leverages third-party shredding services for document disposal in Zoom offices.

Zoom has a Change Management process (available under NDA) that adds oversight, transparency, and control of all changes to the production environment. It establishes guidelines and standards to formally authorize, manage, test, document, monitor, and implement Zoom information system changes in the production environment. All changes are thoroughly tested on staging and testing environments before being rolled into the production environment. Zoom employs a ticketing system for change management that is used to log changes throughout the process, the approval processes include a security review of changes related all areas that require it.

Network logs are collected at the syslog’s system in production. Logs are protected against modification, deletion and/or inappropriate access. Zoom support has access to additional logging for troubleshooting purposes only.

**Customer responsibility**

Logs accessible to Customer admin staff are available in web page format from the Zoom admin portal. Logs can be exported to CSV format as needed. These include operational logs, call logs, Zoom Phone dashboard, and other logs outlined above. Logs that require user ID information will contain the user email and or phone number/extension.
5.2. NCSC Consideration: Vulnerability management

**NCSC Guidance:** Service providers should have a management processes in place to identify, triage and mitigate vulnerabilities. Services which don’t, will quickly become vulnerable to attack using publicly known methods and tools.

**Goals**

*You should have confidence that:*

- Potential new threats, vulnerabilities or exploitation techniques which could affect your 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
- You know service provider timescales for implementing mitigations and are happy with them

**Zoom responsibility**

Zoom has vulnerability management (available under NDA) in place. Zoom performs monthly vulnerability and web application scanning. Scan reports are reviewed by Zoom’s Security and technical teams and discussed with the engineering and development teams. As part of Zoom’s application development process, Zoom performs reviews and testing against OWASP 10 vulnerabilities. Validated findings are tracked in Zoom’s ticketing system throughout remediation. Additionally, Zoom’s security management has subscriptions to US-CERT and are notified about any known vulnerabilities.

Zoom conducts continuous monitoring on its production environment. Production logs and security events are ingested by Zoom’s SIEM tool, which feeds into and generates alerts via Zoom’s ticketing system. Zoom’s Incident Response Plan includes a post-incident review process to provide feedback for continuous improvement on the identification, detection, response and recovery capabilities of security events. Zoom also has a public bug bounty program.

Security personnel are notified when predefined thresholds are met. A ticket is automatically created based on the severity and assigned to a security personnel for further investigation. Zoom leverages various communication means, such as its video conferencing solution, instant messaging, phone, email. Depending on the severity of the event, Zoom employs the available communication means to remediate any issues/events for the production and corporate environment.

Zoom has documented policies based on NIST 800–53, which address vulnerability management. Moreover, Zoom’s Vulnerability Management Standard outlines remediation timeframes for identified vulnerabilities and addresses patch management.

Zooms Incident Response Policy (available under NDA) is established to require the creation and maintenance of a structured Incident Response Plan to guide Zoom’s response to security events, incidents and breaches of the security of Zoom services or the Zoom corporate IT infrastructure. This policy is available under NDA.
Zoom classifies patches as Critical, High, Moderate, and Low. Patch application standards are 7 days, 30 days, 90 days, and 180 days respectively.

5.3. NCSC Consideration: Protective monitoring

**NCSC Guidance:** 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**

You should have confidence that:

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

**Zoom responsibility**

Responsibility for ongoing monitoring (including events and alerts) and acting on exceptions is managed by the NOC and Operations team 24x7. Security incidents are reported and monitored by Security and Operations teams 24x7. Impacts to service status will be updated at Zoom status. Account Owner/Admins will be notified via email of any impact to their account.

Zoom utilizes various tools, technologies, and procedures to monitor and evaluate the performance of our production services (more information available under NDA). Security events and alerts are fed into our Security Information and Event Management (SIEM) system. The SIEM is configured to generate alerts based on pre-set thresholds, warnings and incident events.

In the production environment, Zoom employs a malware/antivirus tool. Additionally, Zoom leverages a next-generation file integrity monitoring (FIM) tool.

In addition to detecting changes to critical system, application, and configuration files in Zoom’s production environment, Zoom’s FIM tool is leveraged to:

- monitor other closely related items such as the registry, installed software, and local users and groups in the production environment;
- detect real-time changes in production;
- quickly identify threats to production systems;
- ensure the availability and integrity of production assets by instantly detecting any changes to production applications and infrastructure; and
- automatically reconcile known vendor updates and patches.

Zoom’s networking team has measures in place to detect and address DoS attacks. Zoom’s networking team is constantly monitoring DoS events, taking action, as necessary.

Zoom has recently implemented protections against meeting ID brute force attacks. Security options to
thwart brute force attacks include: Require participants enter password to join sessions; enable waiting room; separate internal and external participants in the joining process: allow internal employees to join immediately while external participants wait to be admitted or rejected by the meeting host; allow only persons from specific domains. Best practices include not listing meetings as public and sharing meeting ID's via social media.

Customer responsibility
It is possible to monitor the audit logs available through Zoom using the Rest API's, this can then provide further details directly into your own security information and event management tools.

5.4. NCSC Consideration: Incident management

NCSC Guidance: 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.

Goals
You should have confidence that:

- Incident management processes are in place for the service and are actively deployed in response to security incidents
- Pre-defined processes are in place for responding to common types of incident and attack
- A defined process and contact route exists for reporting of security incidents by consumers and external entities
- Security incidents of relevance to you will be reported in acceptable timescales and formats

Zoom responsibility
The incident response program is addressed by the Zoom Incident Response Policy and the Zoom Incident Response Plan, this policy and plan are available under NDA. The Zoom Incident Response Policy has been established to require the creation and maintenance of a structured Incident Response Plan to guide Zoom’s response to security events, incidents and breaches of the security of Zoom services or the Zoom corporate IT infrastructure.

The Zoom Incident Response Plan (IR Plan) defines the minimum requirements for responding to incidents in an efficient and effective manner, including detecting, analysing, prioritizing, and handling of incidents to
(i) determine their scope and risk,
(ii) respond appropriately to the incident,
(iii) communicate the results and risk to all stakeholders, and
(iv) reduce the likelihood of the incident reoccurring.

For breaches affecting a specific customer, Zoom will notify the account owner and administrator(s) through email or as specified in the fully executed service agreement.

Security incidents are reported and monitored by Security and Operations teams 24x7. Impacts to service status will be updated. Account Owner/Admins will be notified via email (or as specified in our
fully executed service agreement) of any impact to their account. Notification of 72 hours is provided when a data breach is confirmed.

Customer responsibility
Incidents can be monitored through Zoom status website and formal responses on the Zoom blog.


**NCSC Guidance:** Where service provider personnel have access to your data and systems you need a high degree of confidence 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**

You should be confident that:

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

**Zoom responsibility**

Zoom has administrative, physical, and technical safeguards and processes in place that prevent unauthorized access to our production environment. Only authorized personnel are allowed access. Access is role-based and least privileged. Access to Zoom's production Infrastructure hosted at AWS requires multi-factor authentication and access to servers hosted by AWS requires secure shell (“SSH”) with private key.

Zoom's HR is responsible for pre-employment screening. All candidates being considered for employment with Zoom are required to complete a background check. Zoom requires all employees to undergo security awareness and privacy training upon hire and yearly thereafter. Zoom ensure that those employees that can interact with the service and data have been fully checked.

For US candidates, the following items are part of the background check process:

- SSN trace, county criminal search (7 years address history), multi-state criminal database search, nationwide sex offender registry search, and OFAC Terrorist watchlist.
- Employment and education verification.

For International candidates, background checks are conducted (if legally permissible by local jurisdiction) and may include:

- OFAC terrorist watchlist, criminal search
- Employment and education verification
Zoom will ensure that no access is permitted without identification or authentication that can be performed on information systems without identification or authentication are identified. Additionally, Zoom has a formal offboarding process in place. Upon termination during the exit interview process, access to Zoom production systems, tools, and the network is removed in accordance with the Access Control policy.

Further details regarding the Personnel security at AWS is available in their AWS 14 Cloud Security Principles. For the co-locations sites does not have the same requirement as all data in these locations is encrypted.

7. NCSC Cloud Security Principle: 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
You should be confident that:

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

Zoom responsibility
Zoom has developed application security standards based on industry best practices for application security development guidelines from OWASP. Zoom has established a formal SDLC process that includes peer code review, testing, static and dynamic code scans, as well as Zoom's formal change management process. Software goes through QA. Testing is done on Zoom's development and testing environments before deployment into production. No customer data is used in Zoom's development and testing environments. Zoom's SDLC is reviewed as part of Zoom's annual SOC 2 audit (available under NDA).

As part of Zoom's application development process, Zoom performs reviews and testing against OWASP 10 vulnerabilities. All third-party applications used as a component of the Zoom services is scanned for vulnerabilities using Zoom's vulnerability management tools. All vendor dependent vulnerabilities are addressed with Zoom's vendors for remediation. This process is tracked through the use of Zoom Plan of Action and Milestones (POAM). Zoom's SDLC includes software composition analysis (SCA) tools and procedures to track and address third-party vulnerabilities and licensing risk.

Zoom performs the activities listed below as part of Zoom SDLC QA process. These tests are performed by individuals that are not developers of the code being tested.

- Manual Test Execution Verification
- Test Automation Development and Execution
Zoom utilizes static code analysis which is implemented as part of Zoom’s SDLC process. Zoom also performs peer reviews for any changes. Security changes are reviewed by the Security team and approved prior to being released into production.

8. NCSC Cloud Security Principle: 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**

You understand and accept:

- How your information is shared with, or accessible to, third party suppliers and their supply chains.
- How the service provider’s procurement processes place security requirements on third party suppliers.
- How the service provider manages security risks from third party suppliers.
- How the service provider manages the conformance of their suppliers with security requirements.
- How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.

**Zoom responsibility**

Zoom has a vendor selection process that examines third-party risk. Zoom evaluates the SOC 2 reports for third-party vendors as part of third-party risk management. Additionally, Zoom engages a third-party auditor to conduct a SOC 2 Type II audit. Zoom utilizes an open source security and license compliance tool, as well as vulnerability scanning tools, for the discovery of possible vulnerabilities.

Additionally, Zoom relies on the following third parties to deliver its Services:
- AWS
- Datacentres/colocations (for real-time communications)
- Internet Service Provider (ISP) and telephony service provider at our datacentres/colocations

Zoom leverages AWS cloud to host its web services. Customer data is stored in AWS.
Zoom’s real-time communications services are hosted globally with tier 3 and above datacentre providers:

- Equinix
- CoreSite
- Digital Realty
- CenturyLink/Level3
- Tata Communications
- Telstra
- Zayo
- Aptum Technologies
- Oracle

Zoom monitors SOC 2 reports and third-party security ratings of key Zoom vendors, sub processors and business partners involved in the processing and storing of customer data. Annual due diligence is performed by Zoom on all critical third parties. As a public company, Zoom also monitors SOC 1 reports for certain third parties who are instrumental in the Zoom service and financial reporting.

Privacy and security requirements for sub processors and customers are addressed via legally binding contractual provisions and data protection agreements.

9. NCSC Cloud Security Principle: 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

9.1. NCSC Consideration: 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.
Goals
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)

Zoom responsibility
Zoom’s support can facilitate ticket intake via phone, online submission, or chat. Zoom’s Technical Support Engineers will follow through on issues to resolution. If needed, escalations are available via your Customer Success Manager.

- Business, Education or API plan subscribers will report support tickets to Zoom by:
  1. Online submission via submit a request.
  2. Chat live with our support team by visiting your account and selecting help in the lower right-hand corner here.
  3. Phone dial-in
     - US: +1.888.799.9666 ext 2
     - AU: +61.1800.768.027 ext 2
     - FR: +33.800.94.64.64 ext 2
     - IN: +91.1800.050.2040 ext 2
     - JP: +81.053.132.0070 ext 2
     - NZ: +64.800.475.039 ext 2
     - SG: +65.800.321.1249 ext 2
     - UK: +44.800.368.7314 ext 2 or +44.20.7039.8961 ext 2

- Pro plan subscribers will report support tickets to Zoom by:
  1. Online submission via submit a request.
  2. Chat live with our support team by visiting your account and selecting help in the lower right-hand corner here.

- Free plan subscribers will report support tickets to Zoom by:
  1. Online submission via submit a request.

When a support ticket is initiated with Zoom’s technical support team, it will be classified according to the following Priority levels:

- Priority 1 - Urgent: 1 hour. The Service is “down,” operation of the Service is severely degraded, or there is a critical impact to the Service due to a fault with the network or other software issue. No workarounds are available. Examples include failures of Zoom’s transmission services or software functions. Zoom will provide necessary resources around the clock to resolve this situation.
- Priority 2 - High: 4 hours. Significant aspects of the Service are negatively affected by inadequate performance of the network or other software issues. Partial or no workarounds available.
Zoom will provide resources during our normal business hours to resolve the situation and additional resources outside of our normal business hours as reasonably necessary.

- Priority 3 - Normal: 24 hours. General issues related to a feature or a set of features. Operational performance of the service is not impaired. Zoom will provide reasonable resources during Zoom’s normal business hours to assist in resolving the problem or providing a workaround.

- Priority 4 – Low: 24 hours. Informational or Feature Change Request: Customer requires information or assistance with service’s capabilities, installation or configuration and there is little to no effect on its business operations. Included are requests for information, assistance, features, alpha/beta and others. Such requests will be handled within Zoom’s normal business hours.

Zoom's back end Operations Portal has role-based access controls and group profiles in place to prevent unauthorized access by Zoom support personnel to user content such as chat and recordings. Technical Support Engineers don’t have access to recordings or chat, but they do have access to meeting metadata and account information.

User Management allows Account Owners and Admins to manage their users, such as add, delete, and assign roles and add-on features. New Users will be sent an activation email. Users with existing free Zoom accounts under the same email address will be sent an email to accept your invitation.

Each user in a Zoom account automatically has a system role, which can be Owner, Administrator, or Member. These roles are associated with a default set of permissions, which cannot be changed for the Owner or Member. These permissions control what users see when they log into the account. Role-based access control enables your account to have additional user roles. User roles can have a set of permissions that allows access only to the pages a user needs to view or edit. In addition, you can change the permissions of Admin system role.

**Customer responsibility**
For additional information on [User Management](#).

For additional information on [Role Based Access](#).

### 9.2. NCSC Consideration: 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.

**Goals**

You 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

**Zoom responsibility**

Each user in a Zoom account automatically has a system role, which can be owner, administrator, or member. These roles are associated with a default set of permissions, which cannot be changed for the owner or member. These permissions control what users to see when they log into the account. Role-based access control enables your account to have additional user roles. User roles can have a set of permissions that allows access only to the pages a user needs to view or edit. In addition, you can change the permissions of admin system role.

Only the account owner can initially create user roles and assign users to those roles. After a user role has been created, the owner (or others in a role with role management permissions) can assign users to that role, granting those users permission to view and edit a subset of pages belonging to the account.

You can see what type of role you currently have on your account profile page. If you are the account owner or admin, you can see what type of role other users on your account have under User Management.

**10. NCSC Cloud Security Principle: 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**

You should have confidence that identity and authentication controls ensure users are authorised to access specific interfaces.
**Zoom responsibility**

Users can access the Zoom portal, Desktop application (Windows, Mac or Linux) and mobile application using either Single Sign-on, Email address and password, Google login or Facebook login. These options can be restricted when deploying the Zoom client to the desktop or mobile devices.

Single sign-on allows you to login using your company credentials. Zoom single sign-on (SSO) is based on SAML 2.0. Zoom acts as the Service Provider (SP) and offers automatic user provisioning. You do not need to register as a user in Zoom. Once Zoom receives a SAML response from the Identity Provider (IdP), it checks if this user exists. If the user does not exist, Zoom can be configured to create a user account automatically with the received name ID.

Using different deployment types, and application configuration software, the Zoom client can be locked down to join meetings hosted by certain accounts and have login restricted to certain domains, and have other settings disabled via remote management.

**Customer responsibility**

Zoom has an enhanced password feature that can require new users to change their passwords upon first sign-in. Customers may enable this in the Zoom portal.

For additional information on Single Sign-on.

---

**11. NCSC Cloud Security Principle: 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**

You:

- understand what physical and logical interfaces your information is available from, and how access to your data is controlled
- have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces ([see Principle 10](#))

**Zoom responsibility**

Zoom provides an admin portal that allows customers to provision, audit, modify, and remove user entitlements. Zoom employs TLS 1.2 for encryption on all sites (this complies with the NCSC guidelines
on TLS), this includes data access through the Zoom web admin portal. In the Zoom admin portal, admins can configure period for inactivity on web (10-120 minutes) and on Zoom Client (5-120 minutes). Also data is protected between services when using the Zoom API’s with TLS 1.2, also the Zoom API’s are using OAuth (Client ID and Client Secret) and JWT (API Key & Secret) to authenticate the API requests.

Zoom is a multi-tenanted hosted application (SaaS), meaning that multiple clients of Zoom access the same application infrastructure. Zoom employs Network Access Controls (NAC) and network monitoring to prevent unauthorized devices from physically connecting to the datacentres and colocations.

Customer data is logically segregated.
1. Each customer will have a unique URL.
2. Each customer has a unique ID, called Account ID. Like UXXXX-XXXX-XXXX. Customer DB records is associated with this account ID.
3. Customer storage top folder name uses Account ID.

Access to Zoom’s production infrastructure hosted at AWS requires multi-factor authentication and access to servers hosted by AWS require secure shell (“SSH”) with private key. For corporate IT, Zoom employs SSO by leveraging an identity management solution to provide centralized authentication and identity management services.

Zoom uses the latest secure serialization & deserialization tool, which is not vulnerable to be used in deserialization attacks and accepting the data from non-trusted sources.

12. NCSC Cloud Security Principle: Secure service administration

**NCSC Guidance:** Systems 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**

*You should:*

- understand which service administration model is being used by the service provider to manage the service
- be content with any risks the service administration model in use brings to your data or use of the service

**Zoom responsibility**

Zoom has a formal Access Control policy in place. Zoom has administrative, physical, and technical safeguards and processes in place that prevent unauthorized access to our production environment. Only authorized personnel are allowed access. Access is role-based and least privileged. Access to
Zoom's production Infrastructure hosted at AWS requires multi-factor authentication and access to servers hosted by AWS requires secure shell ("SSH") with private key.

Access to Zoom's colocation/datacentre servers requires key pair authentication. Remote access to Zoom's datacentre is only allowed through VPN.

Zoom performs full access reviews at least quarterly and any time there is a role change. Moreover, Zoom has a formal onboarding process in place requiring acknowledgment of our information security policies and completion of our security awareness and privacy training. Additionally, Zoom has a formal offboarding process in place. Upon termination during the exit interview process, access to Zoom production systems, tools, and the network is removed in accordance with the Access Control policy.

Administrative actions are logged in the Zoom admin portal under user activity reports. Through integration with the Zoom API, customers can implement custom logs and monitoring (e.g., Dashboard can be used to cross-reference known IPs to participant IPs). Customers can enable enhanced monitoring functionality through API integrations. For more information, please refer to our API documentation on the Zoom Marketplace.

In reference the NCSC System administration architecture, Zoom considers its service as ‘Dedicated devices for community service administration’.

Zoom support team is organised on a global model overseen by a US person, with regional leaders. Support agents are only able to access production records after meeting security requirements following relevant training (as outlined in the SOC 2, available under NDA).

Agents cannot access production code. Agents can read-only access meta data and do not have access to customer content. Agents can only use Zoom provided equipment connected with the corporate network or VPN to perform their roles. All activity is logged and stored in Zoom's OP tools.

Customer responsibility
For more information on Zoom administration.

13. NCSC Cloud Security Principle: 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
You should be:

- aware of the audit information that will be provided to you, how and when it will be made available, the format of the data, and the retention period associated with it
• confident that the audit information available will meet your needs for investigating misuse or incidents

Zoom responsibility
Administrative actions are logged in the Zoom admin portal under user activity reports. Meeting Metadata (Topic, Description (Optional), Participant IP Addresses, Device/Hardware Information, Meeting Statistics/Metrics, Start Time, Join Time, Leave Time) is available in the dashboard.

Reports section of the Zoom website is a powerful tool that provides account owners and admins with various account, meeting, and webinar statistics to review how a customer's organization is utilizing Zoom.

Operation logs contain audit trails of action performed by customer admins users:

- Account configuration/options change
- User changes (add/remove/edit)
- Billing plan change
- IM configuration changes
- Archived Chat access
- Recording management
- webinar settings
- APIs to change Account/User

Failed login attempts are available when users are trying to authenticate using SSO and available in the SAML Response Logs in the Zoom portal. Zoom accounts will lock following invalid password attempts using password authentications.

Customer responsibility
The Zoom Dashboard allows administrators on the account to view information ranging from overall usage to live in-meeting data. This data can be used to analyse issues that may have occurred as well better understand how users are holding meetings within your company. Please refer to the Dashboard article.

Through integration with the Zoom API, customers can implement custom logs and monitoring (e.g., Dashboard can be used to cross-reference known IPs to participant IPs). Customers can enable enhanced monitoring functionality through API integrations. For more information, please refer to our API documentation on the Zoom Marketplace: Introduction and Zoom API.

14. NCSC Cloud Security Principle: 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.

Goals
You:

- understand any service configuration options available to you and the security implications of your choices
- understand the security requirements of your use of the service
- educate your staff using and managing the service in how to do so safely and securely

Zoom responsibility
Zoom places security as the highest priority in the lifecycle operations of its public and hybrid cloud networks. Zoom attains to continually provide a robust set of security features to meet the requirements of businesses for safe and secure HD meetings. Zoom has an information security program that is managed by Zoom’s Chief Information Security Officer (CISO), supported by management and audited by a qualified, independent auditor on an annual basis.

Enforcing SSO access to your Zoom accounts can ensure that only users within your trusted domain can access your user accounts and this can be used to set roles, account settings and services available to your users as well. Adding additional security to your Zoom meeting can also be managed using some of the Account Setting available in the Zoom portal, these include adding restricting access, password, waiting rooms and participant controls available in the meeting.

Zoom has a comprehensive set of information security policies based on industry standards and best practices. Zoom complies with applicable regulatory obligations. For more information, please visit Zoom’s Legal Centre.

Customer responsibility
Securing your meetings is important to Zoom and we have provided the following guide to help with updating your setting to support security best practise:
Best Practises for Securing Your Zoom Meetings

Account Owner/Admins will be notified via email (or as specified in our fully executed service agreement) of any impact to their account.

Please review the Zoom Security White Paper:

Zoom's Terms of Service

Zoom Video Communications GDPR Compliance