Zoom Video Communications Cloud Security Principles (NCSC UK)

July 21, 2020

Approved for Public Release

Introduction

Zoom Video Communications, Inc. ("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.

Applicability

This document applies to UK public sector organizations that contract with or are considering contracting with Zoom for the services referenced herein. This document describes Zoom's services as of the date noticed on the first page. Zoom reserves the right to make changes and updates to its services, systems and environments. Zoom will periodically review and update this document to reflect any such changes and will notice a new publication date at the time of any updated publication.

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 real-time media (audio, video and shared content). Zoom encrypts in-meeting and in-webinar content between each end-user device via the cloud service (data is not decrypted when it is in the Zoom cloud service (The Facts Around Zoom and Encryption for Meetings/Webinars) using TLS and Advanced Encryption Standard (AES) 256-bit.

Encryption keys used to encrypt real-time media are temporarily stored in memory (server and client) and are purged once the meeting ends.

For more details, please refer to the Encryption White Paper (https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf).

APIs: Data in transit is also protected using TLS 1.2 between services when using the Zoom APIs. The Zoom APIs are using OAuth (Client ID and Client Secret) and JWT (API Key & Secret) to authenticate the API requests. More information is available at https://marketplace.zoom.us/docs/guides.

H.323/SIP Devices: When supported and enabled on the device, Zoom will encrypt real-time media (video, audio, and screen share) using AES on a SIP or H.323 endpoints. Specific ciphers vary by manufacturer, model, and firmware version. Zoom supports up to AES-256.

Dial-In Participants: 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.

Chat (Instant Messaging): For chat (instant messaging), 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 read by the intended recipient on an authorized device.

A detailed description of Zoom's encryption can be found in our Encryption White Paper. Please also review the Security White Paper. 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 specific regions. For more information, please refer to https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-hosted-meetings-and-webinars.

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 services. Under the EU's GDPR, Zoom is a "Processor" of Customer Content and Personal Data that its Customers may provide when using Zoom products and services. Zoom customers are the "Controllers". Zoom's Official EU GDPR Compliance statement may be accessed by visiting https://zoom.us/gdpr.

Zoom may store, delete, or disclose such data as directed by the customer. For more information, please refer to https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf.

Zoom leverages AWS to host web services. Zoom's real-time communications services are hosted globally in tier-3 or above data centres.

By default, customer data is persistently stored in AWS in the United States. Zoom has co-located data centres worldwide that are used to facilitate real-time meeting services. Meeting participants are connected to the co-location nearest to their geographic location.

Account owners and admins on paid accounts can customize which data centre regions they use for hosting their real-time meetings and webinar traffic. For more information on this feature, please refer to our support article on selecting data centre regions for hosted meetings and webinars:
https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-hosted-meetings-and-webinars?zcid=1231.

Customer agreements are concluded with Zoom Video Communications, Inc., a US company. Customers may negotiate various terms with Zoom during the contracting process. Zoom also offers a fully GDPR compliant data processing agreement, as referenced above. Further details are available at https://www.zoom.us/privacy.

Customer responsibility

If a customer requires data to be stored within the EU region, that customer may submit this request to Zoom.

Selecting data centre regions for hosted meetings and webinars

Account owners and admins on paid accounts can customize which data centre regions they use for hosting their real-time meetings and webinar traffic. Customers can opt-in or out of each specific data centre region for data in transit. The customer's default region, which is the region where the customer account was provisioned, will be locked (meaning the default region cannot be changed). Additionally, account owners or admins can opt-in for their account to use the China data centre at any time. If customers did not opt-in by April 25, 2020, the customer account will not be able to connect to mainland China for data transit. Users in mainland China will connect to data centres outside of China and therefore may experience performance issues.

Once you opt-out of a region, the regional dial-in numbers will be disabled for your meetings and webinars. Zoom Conference Room Connector (CRC) endpoints in disabled regions will also not be able to connect to your meetings or webinars. Data centre region selections apply

only for meetings and webinar traffic. The selections do not impact the location of data at rest. Data centre region selections also do not apply to Zoom Phone or related features. Even with data centre customization available, Zoom is designed to scale to meet heavy usage demands.

To opt in/opt out now, or to get more information on this feature, please refer to our support article on selecting data centre regions for hosted meetings and webinars: https://support.zoom.us/hc/en-us/articles/360042411451-Selecting-data-center-regions-for-hosted-meetings-and-webinars?zcid=1231.

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 data centre providers. Only authorized personnel have access to Zoom's data centres.

In the data centres, 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 data centres 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 latest SOC 2 report can be shared under a signed NDA.

For the AWS environment, Zoom leverages AWS physical security safeguards. Also, for reference, please see the AWS 14 Cloud Security Principles.

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

Zoom does not transport or store customer data on physical media. Customer data is persistently stored in AWS.

Please see Zoom's Privacy Policy at https://zoom.us/privacy and https://zoom.us/docs/doc/Zoom_GLOBAL_DPA.pdf for a list of data elements processed by Zoom.

Data at rest is protected leveraging Amazon Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256).

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. For more information, please refer to the AWS KMS White Paper.

Zoom performs continuous incremental backups and daily snapshots of the production databases on Amazon AWS. Replicated data is encrypted. AWS Backup secures backups by encrypting data in transit and at rest: https://aws.amazon.com/backup/.

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

Zoom is a SaaS solution; no customer data is stored in removable media. Customer data is stored in AWS. Zoom has an Asset Disposal Policy in place addressing the Zoom data centre

assets, which are wiped or overwritten, prior to being reused. For AWS, Zoom inherits asset disposal controls control from AWS (where customer data is stored).

Zoom has a Data Retention Policy in place. Moreover, Zoom has a process for records retention to ensure that Personal Information is retained for no longer than necessary to fulfill the obligations or meet legal retention requirements. Zoom retains account information only for as long as necessary to comply with legal obligations (e.g., tax compliance) but no longer than 10 years after account termination. 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 with you 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.

Customers can set custom retention periods and delete data as a self-service via in-product features and tools. Dashboard information is automatically deleted on a rolling 12-month period.

Customers are able to delete personal data of meeting and webinar participants as a self-service via in-product tools and technology.

For Zoom Phone: Account owners and admins can set the amount of time that Zoom Phone user data is retained in the system. This data includes call logs, ad hoc/automatic call recordings, voicemail recordings/transcriptions.

Customer responsibility

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

Customers are able to delete personal data of meeting and webinar participants as a self-service via in-product tools and technology.

Account owners and admins can set the amount of time that Zoom Phone user data is retained in the system. This data includes call logs, ad hoc/automatic call recordings, voicemail recordings/transcriptions.

Customers are also responsible for the deletion of local recordings, if enabled: https://support.zoom.us/hc/en-us/articles/201362473-Local-recording.

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. The Asset Disposal Policy addresses the Zoom data centre assets, which are wiped or overwritten, prior to being reused. For AWS, Zoom inherits asset disposal controls from AWS (where customer data is stored).

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

Customer responsibility

Customers are responsible for the security and the security configurations standards implemented on the customer's end-user devices. This includes technical and organizational security measures in the customer's environment that are in scope under the Cloud Security Principles.

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 leverages a robust global network to support its users (both free and paid) natively routing traffic through the meeting zone that will provide the best performance. Zoom has architected the platform such that, in the event of capacity constraints at the data centre nearest a user, additional traffic will be routed to its other data centres.

Data centres are designed to anticipate and tolerate failure while maintaining service levels. Core applications are deployed to an N+1 standard, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

High Availability
Zoom systems are designed and engineered with the goal of minimizing or eliminating critical points of failure. This 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 approach to 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 has a Business Continuity / Disaster Recovery Plan in place. (Available upon request under NDA). Zoom conducts annual testing and review fail-over of its Disaster Recovery (DR) Plan.

SLAs are addressed in Zoom's Master Services Agreement (MSA) and may include 99.9% uptime, excluding excused downtime (maintenance).

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 a software-as-a service (SaaS) provider, 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 logically segregated.

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 follows the recommended security controls established by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Zoom's information security programs are led by Zoom's Chief Information Security Officer (CISO). Zoom has corresponding dedicated security teams for both Zoom Product Security and Zoom Corporate Security. Zoom's information security program addresses the objectives of the program, as well as security standards, guidelines, minimum information security requirements, and baseline controls.

Zoom has a comprehensive set of information security policies based on industry standards and best practices. Zoom's information security policies establish the framework for the security and protection of information, information systems, and security objectives.

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 complies with the following:

- EU-US and Swiss-US Privacy Shield
- GDPR Compliance
- 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. Please visit https://investors.zoom.us/sec-filings for more information.

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

The Zoom Configuration Management Policy (available upon request under NDA) has been established to define Zoom's formal approach to configuration changes as it relates to Zoom's information system. Zoom follows the recommended security controls established by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). NIST CFS is an industry-standard that includes security configuration and hardening standards. Baselines configurations are reviewed as part of Zoom's SOC 2 Type II annual audit.

Moreover, Zoom has a Change Management process 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 to all areas that require it.

Additionally, Zoom has an Asset Management Policy in place. Zoom employs an asset discovery tool in its production environment, which feeds into its CMDB tool.

Customer responsibility

Customers are responsible for the configuration of Zoom settings and Zoom application settings.

Customers are responsible for the security and the security configurations standards implemented on the customer's end-user devices. This includes technical and organizational security measures in the customer's environment that are in scope for this engagement (e.g., mobile device management, identity management, change management, etc.).

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 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. Zoom performs 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.

If a customer believes they have found a security vulnerability within Zoom, please contact Zoom's security team at security@zoom.us.

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 Zoom's 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 https://status.zoom.us/. 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.

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 passcode 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 IDs via social media.

Customer responsibility

It is possible to monitor the audit logs available through Zoom using the Rest APIs. 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: https://marketplace.zoom.us/docs/api-reference/introduction and https://marketplace.zoom.us/docs/api-reference/zoom-api.
This may help provide further details directly into the customer's 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 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 (https://status.zoom.us). 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

Zoom's services status, including any scheduled maintenance and past incidents, is posted on the Zoom Status page at https://status.zoom.us. Customers can subscribe to receive updates.

6. NCSC Cloud Security Principle: Personnel security

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'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 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.

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

Further details regarding the Personnel security at AWS is available in their AWS 14 Cloud Security Principles.

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).

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

Third-Party Suppliers

Zoom uses third-party service providers to help provide and support Zoom services. Zoom discloses these parties as its subprocessors. For more information about Zoom's service

providers, please visit https://zoom.us/subprocessors. Subprocessors only receive data that is needed to provide their services to Zoom. Zoom has agreements with its service providers that say they cannot use any of this data for their own purposes or for the purposes of another third party. Zoom prohibits its service providers from selling data they receive from Zoom or receive on Zoom's behalf. Zoom requires its service providers to use data only in order to perform the services Zoom has hired them to do (unless otherwise required by law). For example, Zoom may use a company to help Zoom provide customer support. The information they may receive as part of providing that support cannot be used by them for anything else.
Zoom may also share data with companies that help Zoom run its business. Examples of these business systems would be accounting systems providers, auditors, etc. This data would be limited to customer account data. User data from the use of Zoom would only be shared with subprocessors in order to provide the service.
As with Zoom's subprocessors, these third parties receive only the information needed to complete their service for Zoom and may not use the data for any other purpose. They may not sell the data.
Zoom does not receive compensation for sharing data with any of these providers.

Third-Party Risk
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.

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. For more information, please refer to https://support.zoom.us/hc/en-us/articles/201362003.

Zoom's backend 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. Zoom customer-supporting teams don't have access to customer content, but they do have access to metadata and account information.

Zoom provides customers with the ability to employ role-based access controls. For additional information, please see https://support.zoom.us/hc/en-us/articles/115001078646-Role-Based-Access-Control.

Customer responsibility

User management allows account owners and admins to manage their users, such as add, delete, and assign roles and add-on features. For additional information, refer to https://support.zoom.us/hc/en-us/articles/201363183-User-Management.

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 the Admin system role.

Only the 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.
Note: Users can only be assigned a single role.

For additional information, please see
https://support.zoom.us/hc/en-us/articles/115001078646-Role-Based-Access-Control.

User and/or Group specific settings can be applied through Group Management in the account to enable/disable certain features and functionality. More information on Group Management can be found here:
https://support.zoom.us/hc/en-us/articles/204519819-Group-Management-.

There are 3 roles in the accounts:

- Owner (all privileges)
- Admin (add, remove, or edit users. Can manage advanced features like Dashboard, API, SSO and Meeting Connector)
- Users (no administrative privileges)

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

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.

Customer 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 can 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 the 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

Zoom supports Single Sign-On (SSO) based on SAML 2.0. In addition to SSO, the Zoom client supports authentication by username and password.

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. For more information, please refer to https://support.zoom.us/hc/en-us/articles/360041019151-Restricting-logins-for-the-Zoom-Client-.

Customer responsibility

The Zoom Client supports Zoom single sign-on (SSO) based on SAML 2.0. Customers can leverage their SSO solution for the implementation of multi-factor authentication (MFA). Zoom acts as the Service Provider (SP) and offers automatic user provisioning. The customer does 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 creates a user account automatically with the received name ID. Zoom can also work with other Service Providers such as PingOne, Okta, Azure, Centrify, Shibboleth, Gluu, G Suite/Google Apps, and OneLogin. Zoom can also work with ADFS 2.0 SAML implementation. More information on our SSO capabilities can be found here: https://support.zoom.us/hc/en-us/sections/200305453-Single-Sign-On and https://support.zoom.us/hc/en-us/articles/201363003-Getting-Started-with-SSO. For more information about SSO with Active Directory, please see https://support.zoom.us/hc/en-us/articles/201363023-SSO-with-Active-Directory.

In addition to SSO, the Zoom client supports authentication by username and password. Meeting passcodes are embedded in the meeting invite URL, so if you click on the meeting invite URL, you will not need to enter a passcode. However, if you join a passcode-protected meeting by directly entering the meeting ID (and not clicking the link), you'll have to manually enter the meeting passcode.

Account administrators can disable the ability to log in to Zoom with an email address and password, requiring users to sign in through SSO or other third-party logins that Zoom offers.

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 is a multi-tenanted hosted application (SaaS), meaning that multiple clients of Zoom access the same application infrastructure. Customer data is logically segregated.

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.

Zoom employs Network Access Controls (NAC) and network monitoring to prevent unauthorized devices from physically connecting to the data centres.

Zoom employs next gen firewall which includes advanced threat protection, which provides:

- Full visibility into all network traffic, including stealthy attempts to evade detection, such as the use of non-standard ports or SSL encryption.
- Attack surface reduction with positive security controls to proactively take away infection vectors.

- Automatic known threat prevention firewall, threat prevention, URL filtering, advanced endpoint protection and a security service, providing defenses against known exploits, malware, malicious URLs and command-and-control (C2) activity.
- Zero-day threat detection and prevention, including threat analytics with high relevance and context.

Customer responsibility

The Zoom Client supports Zoom single sign-on (SSO) based on SAML 2.0. Customers can leverage their SSO solution for the implementation of multi-factor authentication (MFA). Zoom acts as the Service Provider (SP) and offers automatic user provisioning. The customer does 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 creates a user account automatically with the received name ID. Zoom can also work with other Service Providers such as PingOne, Okta, Azure, Centrify, Shibboleth, Gluu, G Suite/Google Apps, and OneLogin. Zoom can also work with ADFS 2.0 SAML implementation.
More information on our SSO capabilities can be found here:
https://support.zoom.us/hc/en-us/sections/200305453-Single-Sign-On and
https://support.zoom.us/hc/en-us/articles/201363003-Getting-Started-with-SSO.
For more information about SSO with Active Directory, please see
https://support.zoom.us/hc/en-us/articles/201363023-SSO-with-Active-Directory.

In addition to SSO, the Zoom client supports authentication by username and password. Meeting passcodes are embedded in the meeting invite URL, so if you click on the meeting invite URL, you will not need to enter a passcode. However, if you join a passcode-protected meeting by directly entering the meeting ID (and not clicking the link), you'll have to manually enter the meeting passcode.

Account administrators can disable the ability to log in to Zoom with an email address and password, requiring users to sign in through SSO or other third-party logins that Zoom offers.

If customers employ passwords as the authentication method in the Zoom client, please see password requirements below:

- Must be at least 8 characters
- Have at least 1 letter (a, b, c...)
- Have at least 1 number (1, 2, 3...)
- Include both uppercase and lowercase letters
- Cannot contain only one character (i.e., "111111" or "aaaaaa")
- Cannot contain consecutive characters (i.e., "123456" or "abcdef")

Please refer to Zoom's support article here:
https://support.zoom.us/hc/en-us/articles/115005166483-Managing-your-password.

Additionally, Zoom has Enhanced Password requirements that can be applied by Admins/Owners of Business-level Zoom accounts. These enhanced options allow customers to:
1. Increase the character requirement (allows for 32 characters maximum).

2. Require letters, numbers, and/or special characters
3. Require upper- and lower-case characters

Customers can also:
1. Force new users to change their password upon first sign-in.
2. Force password expiration in increments of 30, 60, 90, or 120 days
3. Limit the reuse of 3-12 previous passwords.
4. Set the number of times users can change their password within Zoom every 24 hours (Options: ranges from 1 to 8 times; default setting is 3).
5. Force users need to sign in again after a period of inactivity. Set period for inactivity on the web: 10 to 120 minutes (20 is default). Set period for inactivity on Zoom client: 5 to 120 minutes (5 is default)

Accounts are locked for 30 minutes following 6 invalid password attempts. Users may request to reset password by themselves (prior to lockout). Once they are locked out, they can attempt again in 30 minutes or admin may reset it for them at any time.

Moreover, Zoom meetings and webinars can require passcodes for an added layer of security. Passcodes can be set at the individual meeting level or can be enabled at the user, group, or account level for all meetings and webinars. Account owners and admins can also lock passcode settings, to require passcodes for all meetings and webinars on their account. For more information, please refer to https://support.zoom.us/hc/en-us/articles/360033559832.

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.
Remote access to Zoom's production environment requires VPN and MFA. Only authorized Operations personnel are allowed access.

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.

In reference to the NCSC System administration architecture, Zoom considers its service as '*Dedicated devices for community service administration*'.

Zoom's customer-supporting teams have read-only access to metadata and do not have access to customer content or production code.

Customer responsibility

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.

Role-Based Access
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 the Admin system role.

Only the 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.
Note: Users can only be assigned a single role.

For additional information, please see:
https://support.zoom.us/hc/en-us/articles/115001078646-Role-Based-Access-Control.

User and/or Group specific settings can be applied through Group Management in the account to enable/disable certain features and functionality. More information on Group Management

can be found here:
https://support.zoom.us/hc/en-us/articles/204519819-Group-Management-.

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

The 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.

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. Zoom meeting logs are stored and available through Zoom's user portal for six (6) months. Other logs, such as the operation logs, are retained indefinitely.

Operation logs contain audit trails of actions performed by admins:

- 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

Zoom Supports SSO: SSO is supported for sign-on and security. When leveraging SSO to authenticate users, Zoom makes SAML Response Logs available in the Zoom portal.

If customers employ passwords as the authentication method in the Zoom client: Zoom accounts will lock following a predetermined number of invalid password attempts.

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

Security is a priority in the lifecycle operations of Zoom's 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.

Please visit Zoom's Legal Centre for information on Zoom's terms, policies, and compliance: https://zoom.us/legal.

Zoom has a formal documented Zoom Awareness and Training Policy (available upon request under NDA), which defines Zoom's formal approach to security awareness and privacy training for all Zoom employees. Furthermore, Zoom requires all employees to undergo security awareness and privacy training upon hire and yearly thereafter.

Customer responsibility

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.

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

Additional resources:

- Please review the Zoom Security White Paper.
- Zoom's Terms of Service
- Zoom Video Communications GDPR Compliance