FEBRUARY 2025

# Meta Horizon Managed Solutions for Education

## Security and Privacy Whitepaper

Meta

# Contents

# Introduction

As a result of extensive consultation and collaboration with educators, researchers and third-party developers working in the education space around the world, Meta Horizon managed solutions for education includes both the hardware and software to help educational institutions get started with mixed reality and achieve enhanced learning outcomes. We believe it has the potential to transform school lessons, enhance vocational training, and create new opportunities for lifelong learning. Built with privacy and security at the core, it includes essential features like encryption at rest, secure authentication measures, and device and app management controls. Protecting data across **Meta Horizon managed solutions** is our top priority. **Your Customer Data** will not be used for any purposes other than those described in the section of this Whitepaper entitled '**We only use your Customer Data for stated purposes**.'

This whitepaper provides an overview of our security and privacy investments to protect your data.

# A privacy-first approach for our products and services

**Our responsible innovation principles serve as the foundation for all our work. These principles are specifically crafted to protect people's privacy, so educational institutions feel empowered to explore, connect and engage with our products.**

## We provide controls that matter on Meta Quest devices

Meta Horizon managed services for education works with Meta Quest 2, Meta Quest 3, Meta Quest 3S, and Meta Quest Pro, with many core privacy features included on all four headsets. Meta Quest 3, Meta Quest 3S, and Meta Quest Pro have some additional controls over data collection, which are specific to these devices.

### Privacy features common across Meta Quest 2, Meta Quest 3, Meta Quest 3S, and Meta Quest Pro

Several privacy and security features are common to all four headsets. The Privacy Indicator, for example, gives users more visibility into the permissions installed apps are currently using.

Some other examples of common privacy features include:

- Ability to control who sees your information
- Ability to control what data you share with Meta
- Protection of users from visiting websites that are suspected to be potentially dangerous
- Ability to report a bad user
- Information we collect from an end user

In the Privacy Information and Settings section of our Help Center, you can learn about more features.

### Unique sensors and privacy controls for Quest Pro

Released in 2022, Meta Quest Pro was the first Meta Quest headset featuring Natural Facial Expressions (NFE) sensors, and Eye-tracking (ET) sensors. These sensors help power the effect of social presence, which enables people to be their authentic selves in immersive experiences. Along with the introduction of these sensors, we have also introduced additional privacy protections.

For example, **eye tracking** and **natural facial expressions** are off by default and, if turned on, can be paused at any time in the 'Quick Settings' menu. These sensors turn off automatically when the headset is in standby mode. Raw images of people's eyes and face never leave the device, are deleted after processing, and are never shared with Meta or third-party apps. Additionally, people have control over which apps can access ET or NFE sensor data. If the features are not enabled for the device, they cannot be enabled for any app. You can read more about these sensors in the Eye Tracking Privacy Notice and Natural Facial Expressions Privacy Notice.

### Unique privacy control for Meta Quest 3S

Meta Quest 3S includes a Sensor Lock, which automatically turns off your headset's cameras (and microphones) when your headset goes to sleep and turns them back on when the power button is pressed.

### Enhanced mixed reality experiences with Meta Quest 3 and Meta Quest 3S

Mixed reality changes the way people interact with digital content by enabling them to enhance their surroundings without having to leave their environment behind. Mixed reality experiences are powered by spatial data which is collected by the headset and can be used by the device and apps to create unique and sophisticated MR experiences. Meta published a whitepaper on spatial data, which provides details on the different types of data the Meta Quest 3 and Meta Quest 3S collect. It also describes how we applied our responsible innovation principles to minimize any impact to privacy when creating MR experiences for Meta Quest 3 and Meta Quest 3S.

## We protect Customer Data

### We limit access to your Customer Data

Customer Data is the data and content submitted by the Customer or by its authorized users while using Meta Admin Center and the managed Accounts Center.

Meta products serve organizations, educational institutions, and consumers. We know it's important to our customers to have their data separated from end user consumer data. Meta logically separates Customer Data from consumer data, except for permitted data sharing. "Logical separation" refers to a data separation technique used by Meta that applies logic and data tagging in order to separate one or more identifiable data sets from other data sets.

### We only use your Customer Data for stated purposes

Your Customer Data will only be used by Meta (i) to provide and improve the Meta Horizon managed solutions, (ii) for billing purposes, (iii) to promote safety, integrity and security, and (iv) to comply with legal obligations.

Meta may need to share Customer Data with other services, apps, experiences, systems or organizations (i) for billing purposes, (ii) to promote safety, integrity, and security, (iii) to comply with legal obligations, (iv) to perform necessary functions, which includes sharing data with the Meta Horizon OS, and (v) to provide access to other services, apps and experiences permitted by the Customer or its authorized users. When so shared, the specific data that is shared may then be subject to the terms, policies and requirements that apply to such other services, apps, experiences, systems or organizations.

Customer Data will not be used for any purposes other than those described above, including personalization of consumer Meta Products or advertising, and personal data collected from the use of Meta VR Products with a managed Meta account will not be used to personalize ads.

## We set standards for apps on the Meta Horizon Store

Third-party apps available on the Meta Horizon Store are governed by their own terms and privacy policies. We require that developers of those third-party apps abide by the Meta Platform Terms and the Developer Policies, and reserve the right to remove developers or apps that do not fully comply.

We understand that you may sometimes share sensitive information with VR apps on Meta Quest devices. Data processed at the app layer of any third-party VR application is not shared with Meta. The treatment of that data is handled in accordance with the applicable terms of the third-party developer.

## We enable different use modes for Meta Quest devices to meet your educational institution's needs

Meta Quest devices can be configured to either Individual Mode or Shared Mode to enable the configurations and controls that best support your institution's needs. Each mode provides distinct user experiences and data privacy models to suit different use cases.

### Shared Mode

Shared Mode enables multiple people to share Meta Quest devices for easy access to educational institution-curated apps. With Shared Mode, an Admin can determine whether a managed Meta account is required to use the device: if a managed Meta account is required, only users 18 years old or older can use the device; if no managed Meta account is required, users 13 years old or older can use the device. In addition to Shared Mode giving your institution the ability to determine whether an account is required to use the device, Shared Mode provides your institution access to headset configurations that determine app experiences and the ability to assign specific apps to devices . It also allows for further customization of the device's user experiences.

Apps in Shared Mode are accessible to anyone using the device. Shared Mode users can easily cast to people inside and outside of their institution by sharing a web link. Admins can also initiate multiple casts at a time. This is ideal for training and learning environments so educators, faculty, or staff can oversee student activity while they're in-headset.

In Shared Mode, access to the Meta Horizon Store and Meta platform-enabled social experiences, such as messaging, are disabled regardless of whether the user is logged in with a managed Meta account. This ensures your institution is in full control of the apps and experiences available in the headset.

When Admins require login with a managed Meta account to use the device in Shared Mode, educational institutions can still maintain the restricted functionality Shared Mode provides while offering additional capabilities and compatibility with more applications. For example, allowing users to leverage browser-based SSO to sign into apps and creating and using an avatar for apps that require one are possible for users logged in with managed Meta accounts to devices in Shared Mode.

### Individual Mode

Individual Mode enables educational institutions to issue a Meta Quest headset to a single person, similar to device setups for work phones and laptops. In addition, Individual Mode offers admins control over which experiences a person can access, from leveraging the full ecosystem or limiting access to a core set of apps and functionality. Individual Mode utilizes Meta accounts managed by your educational institution, which are only available to those 18 years of age or older. Users in Individual Mode are also able to cast, which allows educators to demonstrate an experience to students before having them jump into mixed reality curriculum.

### Managed Meta accounts and Meta Horizon profiles

When a person 18 years of age or older logs into a Meta Quest device for the first time in Individual Mode, a managed Meta account will be used to authenticate the person and enroll the device into the appropriate mobile device management software. Unlike a consumer Meta account, a person cannot link the managed Meta account to other Meta social accounts (such as Facebook or Instagram) in the Accounts Center.

Meta account information of your educational institution is not visible to users outside your educational institution. Admins can delete a Meta account managed by their educational institutions, which in turn will delete the associated Meta Horizon profile. When they do so, Meta Horizon profile data will be deleted within 90 days, subject to the exceptions provided in the Meta consumer terms and privacy policies.

On first login in Individual Mode, users will be asked to create a Meta Horizon profile. They choose their own username, name, avatar, and profile picture. The Meta Horizon profile determines how people appear in immersive and mixed reality experiences. Meta will have access to the Meta Horizon profile username, name, profile picture, avatar, interactions with games and apps, and list of followers, among other data. This data helps us continue to improve immersive and blended experiences, to enable app functionality, and to use for other purposes as stated in the Meta Terms of Service, the Supplemental Meta Platform Technologies Terms of Service, the Meta Privacy Policy, and the Supplemental Meta Platform Technologies Privacy Policy.

People in an educational institution can download the data associated with their Meta Horizon profile. People in an educational institution can delete their Meta Horizon profile. To delete the associated data, they can delete their Meta Horizon profile. When they do so, Meta Horizon profile data will be deleted within 90 days, subject to the exceptions provided in the Meta consumer terms and privacy policies. Meta Horizon profile data does not include Customer Data associated with a managed Meta account. Customer Data associated with a managed Meta account will not be deleted.

### Individual Mode specific device management controls

Meta Quest Devices in Individual Mode have additional device management controls that empower admins to customize experiences based on their educational institution's needs and constraints.

Admins can:

- Choose to allow people in their educational institution to add a personal Meta account on the Meta Quest device. This may enable them to switch between their personal Meta account and managed Meta account when navigating different experiences on the Meta Quest device.
- Enable or disable access to Meta Horizon Store apps for people in their educational institution. This gives the admin control over the apps people can download and use on the Meta Quest device. Admins can block apps by title, by genre, restrict all mature/17+ content, or restrict all unmanaged content within the store app.
- Decide whether people in their educational institution have access to Meta platform-enabled social experiences, including Horizon Worlds, messaging and more, based on their educational institution's policies.
- Enable people in their educational institution to cast from the device, viewing their experience on the device in real time.
- Choose whether people in the educational institution are allowed to opt in to Meta AI voice assistant.

### FERPA

Educational institutions are responsible under the Family Educational Rights and Privacy Act (FERPA) for securing rights from students or parents (as applicable) to share student data with Meta.

# How Meta Horizon managed services make Meta Quest devices more secure

**Leverage management controls and security features designed to meet common IT requirements in educational institutions.**

## Configure security settings

You can control and monitor your Meta Quest devices and configure them to meet your educational institution's security standards and requirements using the following features:

**Network configuration (VPN support, Wi-Fi)**

The Meta Admin Center offers VPN support for vendors, including Cisco and VMware. Admins can configure a range of Wi-Fi connections, including WPA2 Enterprise (TLS, PEAP), Open & Hidden and disabling MAC address randomization. This allows Meta Quest devices to connect to the institution's Wi-Fi networks.

**OS update controls**

To minimize disruption in your educational institution, admins can choose when and which Meta Quest devices get OS updates. System updates can be applied automatically, delayed up to 30 days or set to a defined time.

**PIN requirements**

Admins can ensure that the Meta Quest device is only used by its assigned person, by enforcing a PIN code every time a device gets unlocked. Admins can set this PIN to be between 4 to 8 characters and even require that no repeating or ordered sequences are used.

Managed services also enable institutions to monitor changes in Meta Quest device security status, and provide:

**Policies and alerts**

Admins can create policies within the Admin Center. Once set, policies trigger automatically and respond to the relevant detected security vulnerabilities by dynamically managing device access and settings. This reduces hands-on work for admins, helps increase security and helps ensure smooth and efficient operations. Admins can also prompt notifications about detected anomalous or malicious activity, and review historical security events in the Admin Center. Policies also help with the protection of devices and can include:

- **Factory reset for detected root access:** If someone gains unauthorized access to your device's operating system (known as "root access"), this policy will wipe the device. This helps maintain the integrity of your device and protect your data.
- **Device quarantine for detected malware:** If malware is detected on a device, this policy will automatically remove company-issued certificates. This helps prevent the spread of malware and protects the rest of your network.
- **Admin notification for insufficient passcode complexity:** If a device's passcode does not meet the required complexity standards, this policy will automatically notify admins, allowing for immediate action to ensure device security.

**Security logs**

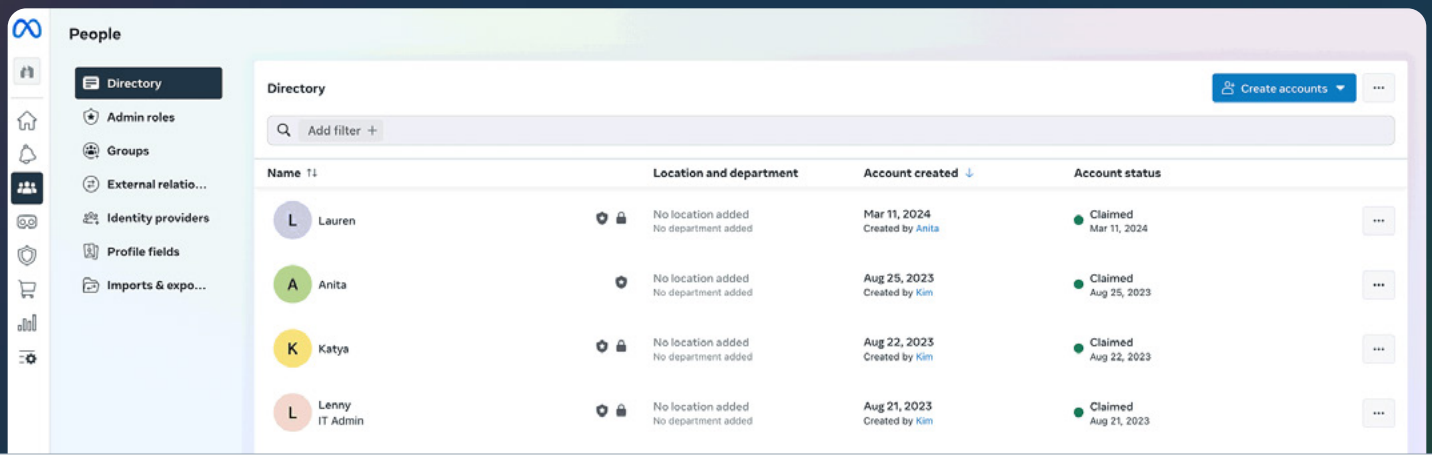
Admins can review security events such as provisioning actions or password changes in the Security Log tab.

**Security logs API**

With the Security logs API, admins can feed Meta security logs into a SIEM or other auditing tool.

**Remote wipe**

Meta Quest devices can be wiped of user and on-device data remotely from the Admin Center or they can be configured to be wiped automatically after a policy is triggered, for example when root access is detected (as described above).




## Enable secure access and authentication[1]

Admins can manage access to Meta Quest headsets from the Admin Center and manage and provision accounts for the educational institution through automated provisioning and integration with major identity providers.

### Managed Meta accounts

Your institution's admin can create managed Meta accounts for people 18 years of age or older to use Meta Quest devices. These managed Meta accounts allow access to the full ecosystem of Meta Quest applications.

### Single sign-on (SSO)

To streamline user access, Meta Quest devices support single sign on. This allows people with a managed Meta account in your educational institution to sign in with their admin-issued credentials.

### Identity integrations

Managed services currently integrate with several identity providers (IdP), including Microsoft Azure AD, Google Workspace Directory and Okta, which offer native app connectors to make SSO and automated provisioning easier. There is support for SAML 2.0 for authentication and a SCIM 2.0 API for automated provisioning, allowing admins to develop custom connectors for account management if the existing identity provider doesn't have a built-in integration. To improve security and reduce the risk of session hijacking, admins can also implement SAML 2.0 single logout (SLO), which ensures people with managed Meta accounts are fully logged out from all sessions, depending on the IdP session.

1. Features discussed in this section apply to headsets configured in Individual Mode. They do not apply to headsets configured in Shared Mode. See below for more information about these configurations.

### Two-factor authentication

Two-factor authentication (2FA) adds an extra layer of security by requiring people with managed Meta accounts to complete a second confirmation step after entering their password when they log in. This reduces the risk of unauthorized access even if the attacker knows their password. 2FA supports various confirmation methods like SMS based, TOTP, security keys and admin-issued codes. Once users with managed Meta accounts have successfully logged in, they have the option to trust a device so they don't have to complete the confirmation step every time they log in from that same device. 2FA is on by default for people logging in with passwords, but they can turn it off if desired.

### Step-Up authentication

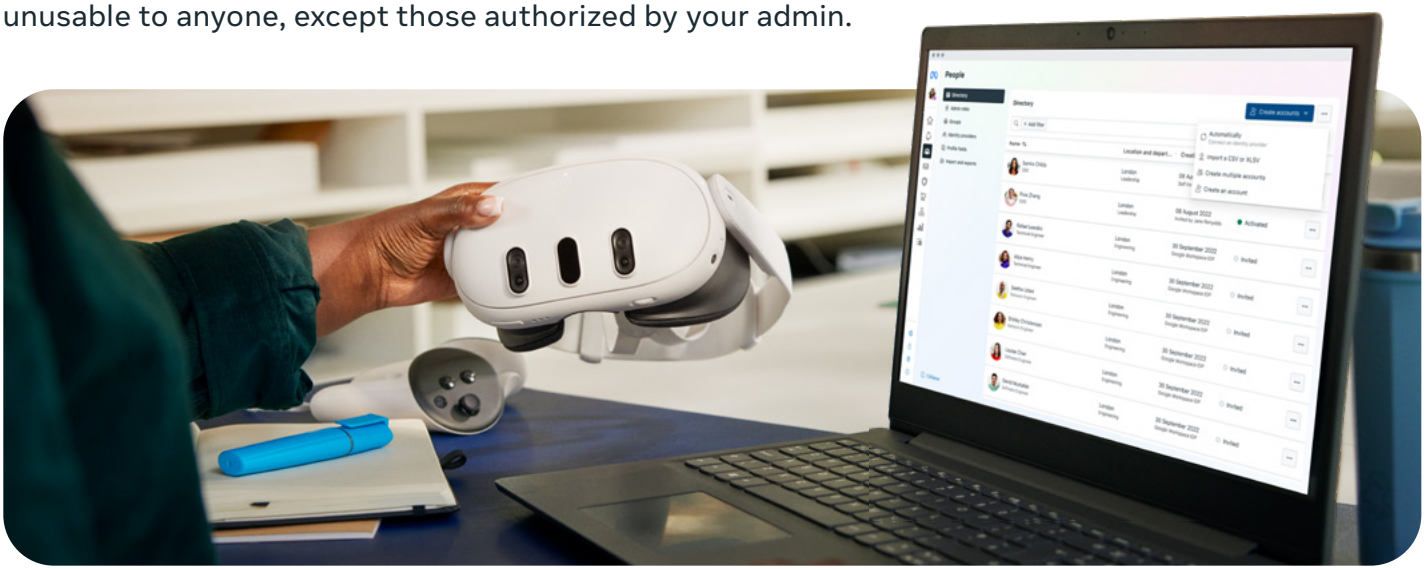
For particularly high-risk actions and transactions, we have added an extra layer of protection, requiring the person to provide additional information to confirm their identity. Examples of high-risk actions include adding or removing admins or changing an educational institution's authentication settings.

### Account and device security

Meta uses a combination of proprietary and open source tools to detect unintended or suspicious IP addresses and devices exposed on the internet. As soon as we suspect that a managed Meta account has been compromised, we lock it and send an email to both the admin and the affected person within the educational institution with steps to recover the account.

When a device is enrolled in your educational institution, the device cannot be set up for use outside of the management of your institution.

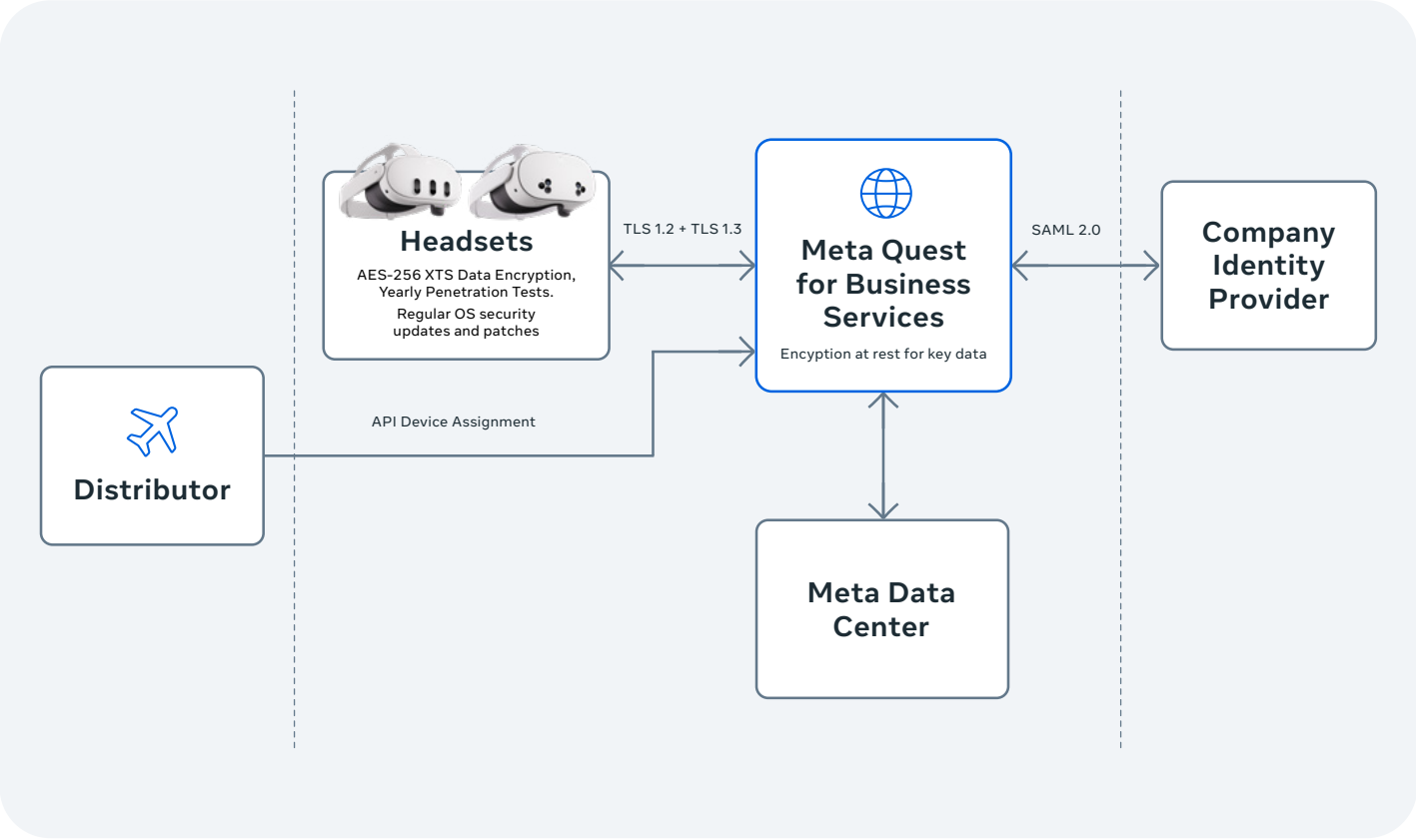
If a device is stolen, and a factory reset is initiated, anyone using the device would need to reconnect to managed services in order to complete the device setup. This makes the device unusable to anyone, except those authorized by your admin.



# We take a multilayered approach to security

**We want you to be confident in the security of your Meta Quest devices, and trust the way we process and store your data, such as data from educators, faculty, staff, and students. In addition to the security capabilities we've built in Meta Horizon managed services, we provide multiple layers of security, from application security to vulnerability management.**

Below illustrates various security elements that come into play in a deployment.




We follow stringent security practices to protect data across our ecosystem, whether it is stored or in transit.

Security is core to how we build our products. This section describes our multilayered approach to security across our software, hardware, applications and operating system. Our security measures include vulnerability management, penetration testing, and encryption.

## Encrypted headset to server transmission

Data transmitted between the headsets and backend servers is encrypted with the industry-standard TLS 1.2 and TLS 1.3 protocols. Certificate pinning on devices and HTTP Strict Transport Security (HSTS) on traditional endpoints where possible is also used. Beyond the headsets' built-in security capabilities, managed services has core device security management capabilities as detailed in How Meta Horizon managed services for education makes Meta Quest devices more secure.

## Encryption at rest

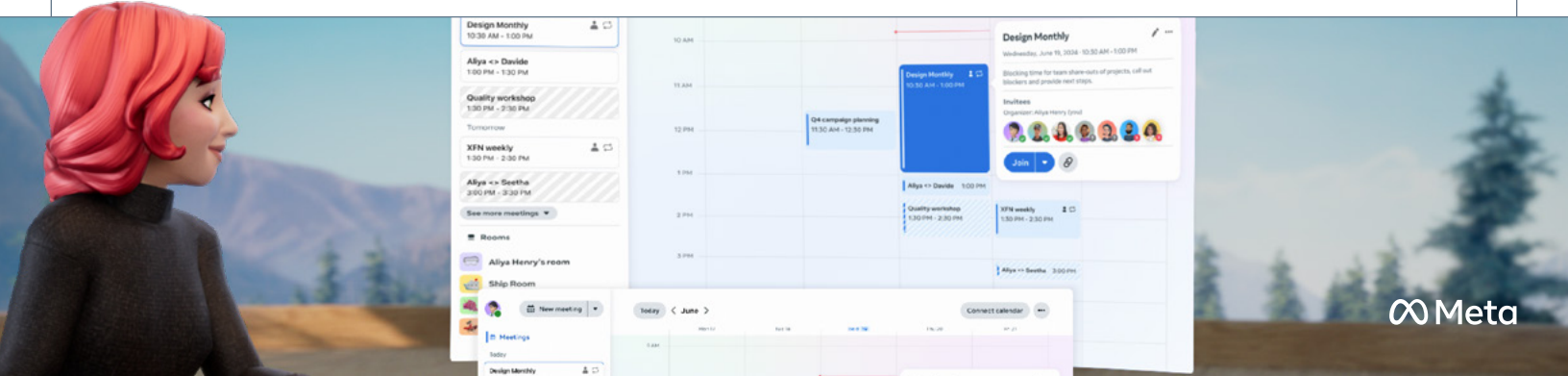
Meta encrypts your institution's key data when it is stored at rest, except for permitted data sharing covered in We only use your Customer Data for stated purposes.

We encrypt your key data before it is persisted in storage. Specifically, this data is encrypted at rest using strong symmetric encryption algorithms such as ChaCha20-Poly1305 (XChaPoly) and AES-GCM. The encryption keys are created and managed by a dedicated service in a secured environment. All access to the encryption keys is logged, ensuring that only entities and systems that need to access your encrypted data stored at rest are able to do so.

## Application security

When people add apps through the Meta Horizon Store, the first line of defense is preventing the installation of malicious and vulnerable apps. Each submitted app must automatically go through the Meta malware detection and vulnerability scanning system. We block apps where we identify potentially malicious behavior.

Store apps are scanned for vulnerabilities through Meta Quest App Static Analysis. The static analysis inspects existing known vulnerability types as well as vulnerable third-party libraries, checking for potential vulnerabilities that may cause apps to be exploited by malicious actors or malware. For example, this analysis detects whether apps are missing certain security checks or using vulnerable versions of third-party libraries. Based on the detection result, the system provides suggestions for developers to fix the issue in their apps. Meta runs security programs to keep malware and app vulnerability detections up to date.



## Malware detection for sideloaded apps

Malware detection for sideloaded apps works by scanning devices to check for the presence of apps from a database of known harmful apps. It uses an APK file hash lookup, which works by comparing the hash of an app file (known as an APK file) on the device with the hashes of known harmful apps in the database. If a match is found, the app is flagged as harmful.

All Meta Quest users with a managed Meta account using the Browser have their URLs scanned by the Safe Browsing system, which is based on Google Chromium Safe Browsing. Meta Quest users will be alerted for potentially harmful URLs which are deceptive or can conduct phishing attacks. People can opt out of this feature in the Browser settings.

## Secure operating system

Meta's Virtual Reality Operating System (VROS) is built on top of the Android Open Source Project (AOSP) and inherits its capabilities. This allows Meta to leverage the security features found in the Android platform. These features include:

- **App sandboxing**
- **App signing**
- **Authentication**
- **Encryption**
- **Keystore**
- **SE Linux**
- **Trusty Trusted Execution Environment (TEE)**
- **Verified Boot**

Meta patches security vulnerabilities in Android OS on a regular basis. Browser patches are also made on a regular basis to help protect the web browsing experience.

## Hardware and firmware security

Meta Quest devices are designed with state-of-the-art hardware and backed by stringent security practices. These devices use the Qualcomm Snapdragon XR2 platform, which contains a separate cryptographic module that supports hardware-backed cryptographic keys. In addition, Meta patches security vulnerabilities in the firmware on a regular basis.

Meta Quest devices follow industry standards in securing devices running Android, including but not limited to:

- Secure Boot which ensures a chain of trust, established in the factory, that all following stacks require.
- Device identity provides uniqueness established in the factory, allowing strong identity for communication with Meta backend services.
- Enforcement mode SELinux implementation locks down critical API access to specific applications.
- Certain data stored on the device, including user account information and all user generated content, is encrypted with industry-standard AES-256 XTS encryption, with optional operating system formatting capabilities if encryption is maliciously disabled.

## Penetration testing

Meta Quest hardware is penetration tested by third-party vendors to ensure no security vulnerabilities escape internal review. New-to-market Meta Quest hardware is tested at least twice. Firstly, for Meta Quest hardware in early development, Meta tests hardware and firmware level security features and implementations including secure boot, anti-rollback, trustzone (TZ) and factory reset/restore. Secondly, later in development, Meta Quest hardware is tested for OS level security and application-level security features, including privilege escalations, secure pairing (accessories), and Out-of-Box-Experience (OoBE) device provisioning. In-market Meta Quest devices are penetration tested periodically to determine if any new features or product updates introduce new security risks and, if they do, we take measures to patch them.

## Vulnerability management

Meta performs regular security and vulnerability testing to assess whether key controls are properly implemented and effective. Meta has a vulnerability management program that includes definition of roles and responsibilities, dedicated ownership of vulnerability monitoring, vulnerability risk assessment and patch deployment.

Meta's security team is responsible for the detection, triage, and remediation of vulnerabilities in Meta Quest hardware and software. Meta leverages various tools to detect security bugs in its code base, as well as in open-source and third-party code, in order to mitigate or fix security bugs before they make it into shipped Meta Quest devices and impact our customers.

## SOC 2 and SOC 3 compliance


Service Organization Control (SOC) is a suite of audit reports provided by the American Institute of Certified Public Accountants (AICPA). These reports are designed to help businesses demonstrate the design and effectiveness of their internal controls related to the services they provide to their customers.

SOC reports provide valuable information to help people assess and address risks associated with an outsourced service. For us, these include:

- **SOC 2 Type I** is a type of audit that assesses our systems to ensure they meet a set criteria across data security, availability and confidentiality. This audit is performed at a specific point in time and focuses on the design of our controls.
- **SOC 2 Type II** goes a step further than Type I. It not only assesses the design of our controls but also their effectiveness over a period of time, typically 12 months. This means that an independent auditor has verified our controls are not only well-designed but also work effectively in practice. Both SOC 2 Type I and Type II are not freely distributed as they are intended for internal use or to be shared with people under an NDA.
- **SOC 3** is a summary report of the SOC 2 Type II audit. It provides a high-level overview of the information contained in the SOC 2 report, but without the detailed descriptions and test results. The SOC 3 report is designed to be a less technical, more user-friendly version of the SOC 2 report. It's like a highlight reel that showcases our commitment to data security and privacy.

Managed Meta accounts have achieved SOC 2 Type I compliance in 2024, and have a corresponding SOC 3 Summary Report.

Read the Managed Meta accounts SOC 3 Report **here**.

Our SOC 2 compliance means we have been audited and found to have satisfactory controls in place to ensure the security, availability and confidentiality of Customer Data. It demonstrates our commitment to protecting Customer Data and maintaining a high level of security standards, giving you peace of mind when you trust us with your critical information.

The report also provides independent validation of our controls and processes, allowing you to assess our capabilities and make informed decisions about your educational institution's security posture. By continuing to work with a SOC 2 compliant provider, you can be confident we are dedicated to maintaining a high level of security and data protection for your institution.

## ISO/IEC Standards

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standard ISO/IEC 27018:2019 is an international standard dedicated to protecting personally identifiable information processed by cloud-based services. This requires an annual external audit to assess Meta's compliance with the ISO 27018 standard to maintain certification. Meta Horizon managed services has completed certification for 2024. A copy of Meta's certificate is available upon request.

## Higher Education Cloud Vendor Assessment Toolkit

The Higher Education Cloud Vendor Assessment Toolkit (HECVAT) was developed by the higher education information security community, EDUCAUSE, Internet2, and the Research & Education Networks Information Sharing & Analysis Center (REN-ISAC). This self-assessment tool aims to standardize the information security and data protection requirements for service providers in the higher education sector. By using HECVAT, institutions can help ensure that their cloud services meet the necessary security and privacy standards, and adopt a consistent methodology for assessing these services.

Meta can provide a completed HECVAT self-assessment. The assessment details our compliance with industry standards and is available upon request.

# Meta Horizon managed solutions for education benefits from Meta's investments in security

**When crafting the security strategy, we tapped into the knowledge available within Meta.**

Meta is a trusted partner to many educational institutions around the world. Our customers trust us because they benefit from Meta's heavy investments in security technology, resilient infrastructure, policies and processes - investments necessary to protect the data of Meta's billions of worldwide users.

## Building security-conscious teams

We understand the commitment to the security of your data starts by hiring the right people and raising their awareness on the importance of data security.

For example, Meta performs background checks on personnel working with your educational institution's instance of Meta Horizon managed solutions for education in accordance with Meta policies, where legally permissible. Meta also ensures all employees with access to Customer Data undergo security training.

## Forming resilient security protocols

Our commitment to the security of your data also manifests through the monitoring, controls and measures we have in place to pre-empt or respond to security risks.

Meta maintains a business continuity plan for responding to emergency or other critical situations that could damage service, and formally reviews the plan at least once a year.

Meta's security measures also include controls designed to provide reasonable assurance that access to physical processing facilities is limited to authorized persons and that environmental controls are established to detect, prevent and control destruction due to environmental hazard. The controls include:

- Protocols requiring personal ID cards for entry to all Meta facilities for all personnel.
- Logging and auditing of all physical access to the data processing facility by employees and contractors.
- Camera surveillance systems at critical entry points to the data processing facility.
- Systems that monitor and control the temperature and humidity for the computer equipment.
- Power supply and backup generators.

## Managing the security lifecycle

Finally, Meta has established and will maintain an Information Security Management System (ISMS) designed to implement industry-standard information security practices. Meta's ISMS is designed to protect against unauthorized access, disclosure, use, loss or alteration of Customer Data.

Meta has a security incident response plan for monitoring, detecting and handling possible incidents. The plan includes the definition of roles and responsibilities, communication protocols and post mortem reviews, including root cause analysis and remediation plans. Meta monitors the service for any security breaches and malicious activity. The monitoring process and detection techniques are designed to detect security incidents according to relevant threats and ongoing threat intelligence.

# Meta partners with and serves respected educational institutions around the world.


# Contact us

For more information about security or anything else related to Meta Horizon managed solutions for education, please **contact us**.

Meta