

Neat Video Collaboration Security and Privacy White Paper

Updated August 2026

In today's interconnected world, security and privacy are paramount for video collaboration. This white paper details the comprehensive, multi-layered security framework and privacy-first approach embedded within Neat Video Collaboration Solutions. From the hardened Neat OS—built upon the Android Open Source Project (AOSP)—to our strict adherence to Secure Development Lifecycle (SDL) practices, Neat is committed to providing a reliable, functional, and secure communication experience for every customer. We outline our foundational security standards, operational practices, and proactive vulnerability management designed to protect both system integrity and user data.

In addition to these broader security and privacy standards, this white paper provides information on the integration and operation of Neat devices within our core software platform providers - Microsoft Teams Rooms, Zoom Rooms, and Google Meet Rooms.

Table of Contents

Secure and Hardened Embedded Operating System **3**
- **Core Pillars of Neat OS Multi-Layered Security** **3**
- **Security Standards and Protocols** **4**
- **Security Features of Neat Devices** **4**

High Level Device Architecture **5**
Software Distribution **6**
Secure APIs **6**
Vulnerability Management, Security Audits & Pen-testing **6**
Device Model and Android Operating System Matrix **6**
Secure Development Lifecycle (SDL) Practices **7**
- **Architecture and Design (Planning)** **7**
- **Implementation & Testing** **8**
- **Release Management** **8**
- **Ongoing Product Maintenance, Security, and Updates** **9**

Device Analytics **10**
Privacy Statement Regarding Data Collection **10**
Incident Response & Breach Notification **10**
Certifications / Attestations **11**
Software Platform Provider Specifics **11**
- General 11
- **Microsoft Teams Rooms** **11**
- **Zoom Rooms** **12**
- **Google Meet Rooms** **12**

Additional Resources **14**
- **Proprietary Information and Disclaimer** **14**
- **Intended Audience and Distribution** **14**

Secure and Hardened Embedded Operating System

Neat OS, the operating system for Neat devices, is built upon the Android Open Source Project (AOSP). It is a hardened and secure platform specifically engineered to support a wide range of audio and video meeting collaboration applications, guaranteeing a consistently reliable meeting experience. All Neat hardware devices run our Neat OS.

Neat OS, a product of close collaboration between Neat's R&D hardware and software engineers, provides a foundation for secure video collaboration. This synergy ensures an optimal blend of compatibility, functionality, reliability, and security for Neat's embedded system appliances in any operational environment.

To safeguard user privacy and system integrity, Neat OS is engineered with a rigorous, multi-layered security framework that operates from startup through continuous operation. This comprehensive approach is designed to eliminate vulnerabilities and provide a trustworthy platform for all communication.

Core Pillars of Neat OS Multi-Layered Security

The security architecture of Neat OS is built upon several foundational components:

- **Secure Startup**: Tamper-Proof Initialization
  The system's integrity is verified from the first instruction. Hardware-backed secure boot and verified boot ensure that only authorized, untampered software is loaded, preventing rootkits and persistent malware from compromising the OS before it starts.

- **Data Protection**: Encrypted Privacy
  Sensitive user data, including configuration files and local logs, is protected using robust encryption mechanisms like File-Based Encryption (FBE) and TLS 1.2/1.3 for data in transit. This ensures privacy both at rest and in transit.

- **Software Integrity**: Anti-Rollback Protection
  Anti-rollback protection prevents intentional or accidental downgrades to older, potentially vulnerable software versions, ensuring the system always runs with the latest security patches and protections.

- **Key Storage**: Hardware-Backed Cryptography
  Critical cryptographic keys for encryption and authentication are stored in a hardware-backed keystore (located in a Trusted Execution Environment (TEE). This isolates keys from the main operating system memory, protecting them from software-based attacks.

- **Access Control**: Principle of Least Privilege
  The system utilizes SELinux (Security-Enhanced Linux), a powerful Mandatory Access

Control (MAC) system. SELinux defines detailed, non-discretionary access rules, effectively sandboxing processes and rigorously restricting their access only to the system resources required for their function.

Security Standards and Protocols

Neat OS adheres to enterprise-grade security standards:

- **Encryption**: TLS 1.2/1.3 for data in transit and File-Based Encryption (FBE) for data at rest. Neat Share utilizes RTP over TCP + TLS 1.2+.
- **Authentication**: Supports 802.1x (EAP) for enterprise network authentication and integrates with enterprise identity management systems. The web interface also requires a secure login when enabled.
- **Operating System Security**: Based on AOSP, the OS includes hardware-backed secure boot, user data encryption, and SELinux.
- **Device Identity**: Each device receives a unique digital certificate at the factory, which serves as a hardware-based ID for secure machine-to-machine (M2M) communication.
- **Network Security**: Where applicable, support WPA3/WPA2/WPA, WEP, and WPA/WPA2/WPA3-Personal Wi-Fi protocols, along with secure web management access over TLS 1.2+.
- **Device Pairing**: Initial setup uses specific network ports, but all ongoing communication between paired devices is fully encrypted (using web traffic on TCP port 8443) to prevent eavesdropping and unauthorized access.

Security Features of Neat Devices

Neat devices are designed with a focus on security and limited access:

- **No Google Mobile Services (GMS):** Neat devices do not run GMS, which includes applications and services like the Google Play Store, Search, and Chrome.
- **Restricted Operating System Access:** The Neat firmware is designed to prevent users from accessing the operating system or components outside of the designated user experience.
- **Android Debug Bridge (ADB) Disabled:** ADB, a command-line tool for administrative functions, app installation, and shell access, is disabled and locked by design on all devices running Neat's release software.
- **No Personal Data Storage:** Neat devices do not store personal data. For personal data stored by third-party applications (e.g., Microsoft), users should contact the application

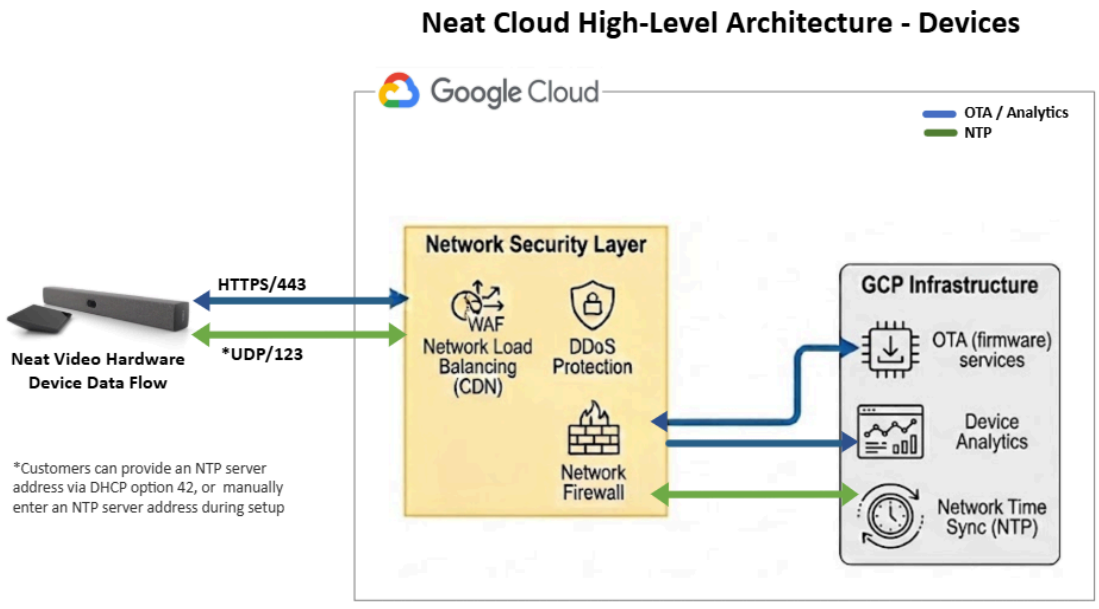
provider.

- **Physical Security:** Neat Bar, Neat Bar Pro, Neat Frame, and Neat Pad include integrated security lock slots for added physical protection.
- **Limited USB Functionality:**
    - The Neat Android Operating System (OS) includes a very narrow set of essential USB drivers and is stripped of unnecessary services like file managers that could be used to copy and run executables.
    - Drivers for USB mass storage (e.g., flash drives) are not present, preventing their use for transferring malware.
    - USB usage is limited to specific use cases: standard keyboard/mouse, touchscreen capabilities, USB headsets, and USB-to-Ethernet adapters.
    - The system will enumerate a connected USB device, but it will not operate unless its driver is explicitly included in the OS device driver list. This minimal support significantly reduces the risk of attacks from malicious USB payloads.

High Level Device Architecture

This section provides a high-level, logical overview of device-dependent services hosted in Google Cloud Platform. The diagram illustrates the service components, communication protocols, and access management controls.

Refer to the following support article for details on the network and firewall requirements for all Neat products.



Software Distribution

Platform vendors (Microsoft, Zoom, and Google) provide the relevant APKs to Neat. Neat includes these software APKs in its total software package and tests them thoroughly before this is released as a bundle to the customer. Neat does not have access to the source code of vendor APKs. Platform vendors are responsible for these packages, and any security concerns towards these APKs should be addressed to Platform vendors directly.

Updates for both Neat firmware and Platform vendors software are available in two ways. By default, Neat products are configured to auto-update to ensure devices are always up to date and include the latest security features. It is also possible to opt-out of Neat's auto-update functionality and update Neat products manually from Neat Pulse or the Platform vendors portal.

Secure APIs

Public APIs are not available on Neat devices. The only API available is the Web API that is used for remote administration (if enabled) and for a Neat Pad controller/scheduler. In this scenario, authentication uses a JWT (JSON Web Token).

The JWT is valid for the lifetime of the Neat product. Lifetime validity of the JWT is required to maintain pairing between a Neat Bar, Bar Pro, or Board (or other Neat device) and the Neat Pad controller/scheduler allowing the room system to operate without downtime. This also helps when there is a reboot, and will allow the Neat Pad to automatically pair with the associated Neat device.

Vulnerability Management, Security Audits & Pen-testing

Our security team continuously monitors and analyzes security risks to Neat devices. If we discover any security vulnerabilities that directly affect our products, we will work on resolving those issues quickly and release patches to our customers through our standard software update channels.

Neat engages independent security consultants to conduct audits and assessments of the Neat Bar and Neat Pad devices. Testing is performed on production hardware with

production (user) builds of device software. All issues observed are remediated and retested to ensure the devices are secure. A summary report of the latest test can be made available upon request.

Device Model and Android Operating System Matrix

The matrix below lists the Neat device model along with the supported version of the Android operating system (AOSP).

Neat Bars

Model	AOSP Version
Neat Bar	10
Neat Bar Gen 2	13
Neat Bar Pro	13

Neat Boards

Model	AOSP Version
Neat Board 32	15
Neat Board 50	13
Neat Board Pro	13

Companion Devices

Model	AOSP Version
Neat Pad	13
Neat Pad Pro	15
Neat Center	15
Neat Frame	13

Secure Development Lifecycle (SDL) Practices

Neat's devices are designed with a modern security and privacy-first approach, drawing inspiration from standards like ISO/IEC 27001:2022 and NIST SP 800-53 Rev. 5. This commitment is formalized through adherence to Secure Development Lifecycle (SDL) practices, encompassing architecture and design, implementation and testing, release management, and ongoing maintenance.

The entire SDL process is managed within a dedicated project management and issue tracking platform, ensuring clear prioritization and the highest quality standards for Neat products.

Architecture and Design (Planning)

This initial stage involves a comprehensive review of the application structure, usage scenarios, and third-party dependencies, including hardware components.

- Risk Profiling and Threat Modeling: The development team, in coordination with the CISO/Security team, prepares a risk profile. This identifies potential attacker entry points (e.g., web interface API, I/O ports) and categorizes security risks based on their severity, impact, and likelihood.

- Defining Secure Architecture: Based on the risk profile and threat modeling, the team determines key secure software architecture components (e.g., user interface, application partitioning) and necessary security features, such as cryptography, audit/logging, and user identification. Test cases for subsequent stages are also defined here.

- Security Risk Assessments: For major updates or significant architectural changes, the CISO/Security Team performs a documented security risk assessment. This may include reviewing design documents, systems analysis, application architecture, a privacy impact assessment (if required), and a formal threat modeling exercise.

Implementation & Testing

This phase focuses on writing and stabilizing application code while building security directly into the product.

- Secure Coding Practices: Neat enforces secure coding practices to mitigate high-risk vulnerabilities, mandates the use of secure development tools (libraries, frameworks), and implements checklist-based code peer reviews and automated/scripted code reviews. Secure code reviews actively reduce potential firmware security issues.

- Firmware and Code Integrity: To protect code from unauthorized access and tampering, it is stored in secure, restricted repositories. Version control tracks all code changes, and only trusted certificate authorities are used for code signing and software distribution, ensuring firmware integrity up to the customer environment.

- Vulnerability Monitoring: Third-party components, including those sourced from the Android Open-Source Project (AOSP), the upstream Linux kernel, and System-on-Chip (SOC) manufacturers, are continually monitored for vulnerabilities, and updates are applied as necessary.

- Independent Security Testing: Separate from the core development effort, the security team, led by the CISO, performs both network and application-level vulnerability testing. Regular vulnerability scans are conducted to ensure releases are free from significant or critical security issues, with all discoveries reported back for immediate prioritization and remediation tracking.

Release Management

Neat employs a formal release procedure to protect software integrity throughout the release

train.

- Environment Separation and Access Control: Strict separation is maintained between development, testing, and operational environments. Strong access controls ensure that employees can only access job-relevant data, preventing unauthorized code changes while maintaining development velocity.
- Version Control: A clear and effective version control methodology is used to track the source and time of every code alteration.
- Final Security Review: After quality assurance and testing phases, a final security review and re-testing are performed before the firmware is deployed to the available customer upgrade channels (preview or stable).

Note: Neat does not bundle application provider application updates with its firmware releases. By default, devices are set to automatically update to the latest stable release.

Ongoing Product Maintenance, Security, and Updates

Beyond the initial release and regular feature enhancements and bug fixes, the product lifecycle includes a crucial maintenance stage focused on the long-term security and stability of Neat video collaboration solutions. This involves a proactive approach to monitoring, integrating, and distributing security updates.

- Regular Security Patch Integration: We commit to a consistent process for reviewing and integrating security patches, particularly those related to the Android operating system which forms the foundation of our devices. These patches are incorporated into our standard software development lifecycle, undergoing rigorous testing before being distributed to all Neat devices through the established, reliable firmware release process. This ensures that devices are continually protected against known vulnerabilities.
- Emergency Vulnerability Response: Should a critical, high-impact security vulnerability be identified that poses an immediate threat to our customers, Neat has an established protocol for rapid response. In such cases, the standard release cadence is accelerated, and an emergency, out-of-band firmware release is made immediately available to all Neat customers globally. This ensures the fastest possible remediation of the critical issue and minimizes potential exposure.
- Life Cycle Management: Our commitment to security extends throughout the supported life cycle of each product. This ongoing vigilance and regular update schedule provide customers with the confidence that their video collaboration environment remains secure, compliant, and operational for the long term.
- Security Testing: To maintain the highest level of security, Neat regularly hires independent security consultants to perform assessments, attestations, and penetration testing of Neat video devices and Neat Pulse services. All identified issues are fully resolved and retested to confirm the devices remain secure.

Device Analytics

To improve product performance and provide a personalized user experience, the following categories of device analytics are collected and transferred to our secure servers:

- **System Configuration:** Firmware channel, build number, and device up-time.
- **Identification & Connectivity:** Serial number and pairing information.
- **Preferences & Localization:** Audio settings and locale (language and country).
- **Third-Party Integration:** App provider details.

Privacy Statement Regarding Data Collection

Our devices are designed with privacy in mind and do not collect, store, or transmit Personally Identifiable Information (PII). However, please be aware that third-party applications such as Microsoft Teams, Zoom, and Google Meet may store sensitive information within their respective cloud infrastructures. We strongly recommend reviewing the data privacy policies of these application providers to understand how your information is handled.

Additionally, while our system logs are encrypted, they may contain IP addresses or hostnames, which could potentially be associated with PII depending on your network configuration and usage context.

Neat Pulse will process Customer Personal Data solely for the purpose of delivering the Services, which include user provisioning, device provisioning, device management, etc. Further details regarding data transfer and processing can be found at Data-Processing-Addendum.pdf.

Incident Response & Breach Notification

Neat has a defined Security Incident Response plan detailing the procedures for addressing computer security incidents affecting Neat products and internal information systems.

Key elements of this plan include:

- Identifying incident response stakeholders, their roles, and responsibilities.
- Defining incident triggering sources, types, and severity levels.
- Establishing requirements for testing, post-incident analysis (lessons learned), and collecting metrics to assess response effectiveness.

Should a data breach occur that could potentially impact sensitive customer data, Neat will promptly notify the affected customer(s) via email of any actual or alleged incident involving unauthorized or accidental disclosure of, or access to, any personal data or other breaches.

Customers who need to report a security concern regarding a Neat device can do so by visiting Neat's security vulnerability reporting policy page: https://support.neat.no/article/security-vulnerability-reporting-policy-at-neat/.

Certifications / Attestations

Neat's achievement of the ISO/IEC 27001:2022 certification underscores its dedication to upholding a world-class Information Security Management System (ISMS). This certification rigorously confirms that our security practices are comprehensive and align with global industry standards. Critically, the scope of our ISO 27001 certification includes all Neat products and services, encompassing both our physical devices and the Neat Pulse device management platform, ensuring a consistent and high level of security assurance across our entire offering. We are dedicated to continually expanding our security posture, leveraging ISO 27001 as the foundational security standard framework for both the company and the secure development of all our future products and services.

Software Platform Provider Specifics

General

Default admin password

The default admin password for a Neat video device running is the last six digits of the device's serial number. For example, if your device's serial number is NA00000XXXXXX, the default password is XXXXXX. You can typically find the serial number on a sticker on the physical device or within the Neat settings menu under Devices. Where a Neat device ships with a default administrative password, that password should be changed immediately on first sign-in, or set and enforced centrally through Neat Pulse. Neat recommends managing device passwords via Neat Pulse for consistent policy across a fleet.
This applies to Neat devices running Microsoft Teams Rooms, Google Meet, and Neat Open mode. Zoom Rooms uses a different access model — see the Zoom Rooms section below.

Microsoft Teams Rooms

Security and Microsoft Teams

Microsoft Teams data is encrypted in transit and at rest in Microsoft services, between services, and between clients and services. Microsoft does this using industry standard technologies such

as TLS and SRTP to encrypt all data in transit. Data in transit includes messages, files, meetings, and other content.

TCP data flows are encrypted using TLS, MTLS, and Service-to-Service OAuth protocols that provide endpoint authenticated communications between services, systems, and clients. Microsoft Teams utilizes these protocols to create a network of trusted systems and to ensure that all communication over that network is encrypted.

For more information refer to Microsoft's Security Guide for Teams.

Meeting Room Guidance for Microsoft Teams

The articles referenced below are intended to guide users on how to optimize meeting spaces with Microsoft Teams Rooms (MTRs) solutions operating on Neat devices.

- How to setup Microsoft Teams Rooms
- Overview of features supported by Microsoft Teams panels
- Authentication best practices for Teams shared device management on Android devices
- Conditional Access and Intune compliance for Microsoft Teams Rooms
- Supported Conditional Access and Intune device compliance policies for Microsoft Teams Rooms

Zoom Rooms

On a Neat device running Zoom Rooms, access to the device System menu is governed by the Zoom Rooms passcode configured in the Zoom portal. A separate Neat-level device password is optional and can be enabled and managed through Neat Pulse.

The articles referenced below are intended to guide users on how to optimize meeting spaces with Zoom Rooms solutions operating on Neat devices.

- Follow These Key Dos and Don'ts to Help Secure Your Zoom Room
- Zoom and Neat System Settings
- How do I setup a calendar for a Zoom Room?
- Zoom Meeting Security Guide

Google Meet Rooms

The articles referenced below are intended to guide users on how to optimize meeting spaces with Zoom Rooms solutions operating on Neat devices.

- Assign a Google Calendar to Meet hardware | Set up & manage services
- Manage Google Meet hardware - Google Workspace Admin Help
- Google Meet security & privacy for IT admins
- Google Meet Security & Privacy for users

Additional Resources

We encourage you to visit our support website and view new articles, FAQs, how-to and troubleshooting guides which are being regularly added there. Please search the following page to find answers to your common questions or problems: https://support.neat.no

If you encounter an issue with your Neat device or service, you can open a ticket in Pulse at https://pulse.neat.no. Customers can submit a ticket directly from their device/room or the portal).

Proprietary Information and Disclaimer

This document, detailing the specifications and information regarding Neat's services, is the property of Neat and is subject to change without prior notice. Neat is responsible for its creation and maintenance.

While all statements, information, and recommendations within this document are believed to be accurate, they are provided *without* any warranty, express or implied.

This document does not constitute a formal agreement. Neat explicitly disclaims liability for any damages, including, but not limited to, lost profits, loss of business, or any consequential, indirect, special, incidental, or punitive damages arising from or related to this document.

Intended Audience and Distribution

This document is intended strictly for Neat's partners and customers. Unauthorized distribution is prohibited and requires explicit permission from Neat.