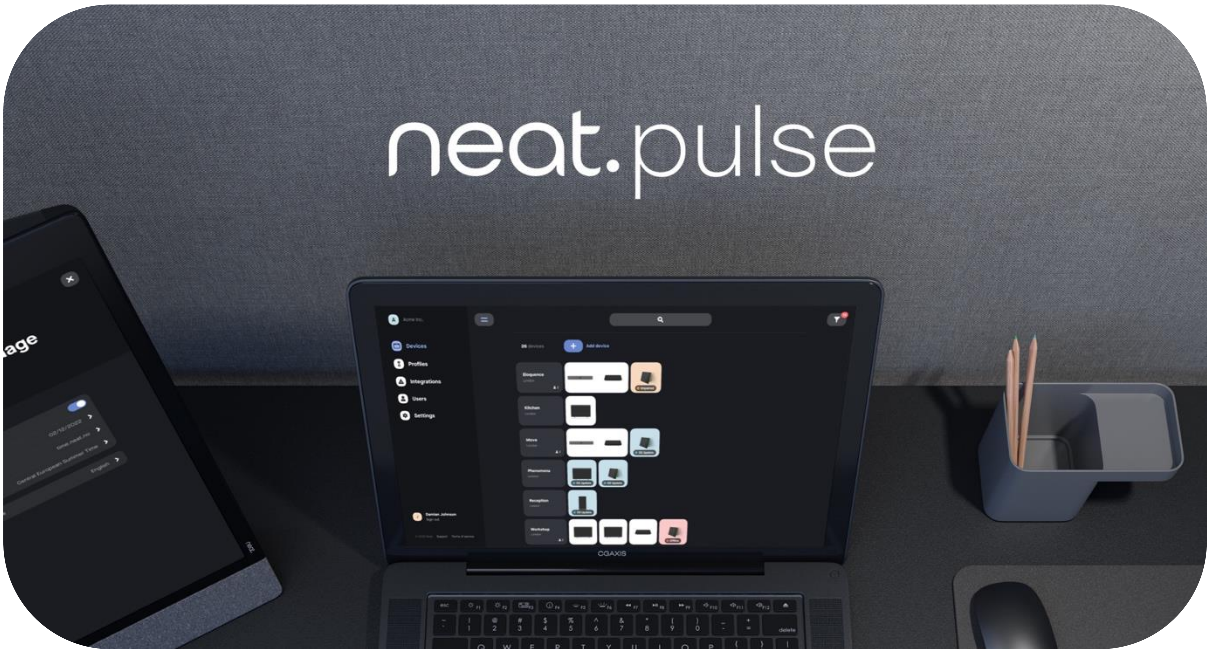
Neat Pulse Security Whitepaper



Last updated July 2025

Introduction

This whitepaper describes security information for the Neat Pulse service. Security is important to us, and we continue to invest in tools, processes and technologies to keep our customers, partners, and their networks safe. This includes implementing information security controls, safeguarding data, and ensuring overall availability of Neat Pulse services.

Neat Pulse provides customers and partners with a secure web portal for enrolling and managing their Neat devices. Customers and partners have the ability to modify device configuration settings, update firmware, run reports, and perform other device management functions.

Neat Pulse has been designed from the ground up with a modern security and privacy perspective in mind, taking inspiration and following guidelines from standards such as ISO/IEC 27001:2022 and NIST SP 800-53 Rev. 5. Care is taken through the entire software development lifecycle: from initial concepts, through design, implementation, testing, to change management and release. Backing up the processes and procedures are a set of stakeholders experienced in building high quality secure systems.

User & Device Access

Users authenticate to Pulse via Microsoft Azure B2C allowing both single sign-on (SSO) and traditional username/password login methods. The Pulse Azure B2C implementation supports multiple identity providers, including Microsoft Entra ID and Google Identity Services. Most importantly, no passwords or password hashes are ever stored by Pulse. This allows customers to login into Pulse without having to share their credentials with Neat. Pulse stores a reference to the Microsoft data for purposes of authorizing logins - but limits any user-specific metadata to the minimum required for functionality.

Neat Pulse supports integration with Identity Providers (IdPs) using SAML for SSO. This allows organizations to use their existing IdP infrastructure (e.g., Entra ID, Okta, etc.) to manage user authentication for Neat Pulse and enabling centralized identity management and simplifying user access.

Azure B2C password rules are set to *strong complexity* which requires a password that's at least 8 to 64 characters and contains 3 out of 4 of lowercase, uppercase, numbers, or symbols.

Devices are enrolled into Pulse using a randomly generated code provided within the Pulse administration portal. The code will be available until a device is registered (no timeout). Once a code is used to enroll a new device into the platform, the code will be auto expired within 8 hours. After enrollment into Pulse, the device is assigned a secure, secret key, which is used to authenticate the device for future communications.

Authorizations / Roles

Administration of Pulse is performed by two user roles - Owner and Admin.

- Owner: Owners have access to all settings in the organization. There can be multiple owners by organization. Owners can invite others to the platform.

- Admin: Access for admins is restricted to specific regions. Admins can only administer endpoints within these regions and cannot edit profiles. Admins cannot add users and edit organization settings.

Owner accounts in Pulse Control will have the ability to use the remote control feature on any device enrolled to their organization, and admin accounts in Pulse Control will have the ability to use the remote control feature on any devices set up in their admin region. Neat support personnel need to be invited by a customer into their Pulse instance for troubleshooting purposes.

Networking and Firewall

Device Requirements

For a device to enroll in, and maintain connection to, Pulse, they require working HTTPS connections to the Pulse cloud service and working DNS to look this service up.

Protocols required for Pulse operation:

- HTTPS, including HTTP/2 and HTTP/1 with WebSockets
- DNS

DNS hostnames:

- pulse.neat.no
- *.pulse.neat.no

IP addresses:

- 20.76.42.235
- 20.16.158.114
- 108.142.134.73
- 13.81.211.248

Ports:

- 443 TCP

HTTP proxies are supported if they support “HTTP CONNECT”.

The list of IP addresses above is subject to change.

Refer to the network and firewall requirements article on Neat’s Support site for more details (https://support.neat.no/article/network-and-firewall-requirements-for-neat/).

Data Security

In-Transit

Data transferred to and from Neat Pulse always utilizes HTTPS with TLS v1.2 or above. There are two separate types of connections to Neat Pulse: a user navigating to pulse in their browser and the pulse agent on Neat devices. In each case, the same protocols and approach to security is used, minimizing the Internet-facing surface area of the product. Attempts to access the service as HTTP are immediately upgraded to HTTPS, ensuring all connections are encrypted.

TLS certificates and cipher suites are regularly reviewed and checked with third-party security reports including Qualys SSL Checker. TLS certificates are managed with best practices such as short expiration dates and weekly renewal. Cipher suites are updated according to industry guidelines; AES 128/256 or ChaCha20.

At-Rest

All data stored on the Pulse cloud service is encrypted at rest using AES 256-bit encryption. This includes all databases, image files, log files, and more. This data is stored on Microsoft Azure servers. There is no physical server access available outside of that which is used by the cloud provider.

Data Backup and Retention

Pulse backups are managed by the built-in Microsoft Azure Backups as well as customized backup jobs run by the Pulse operations team. The custom backups are encrypted and stored in a separate location in Azure and are performed daily. Backups are retained for up to 30 days. The database used maintains three local redundant synchronous copies of the database files to ensure data durability. Where appropriate, high availability (HA) architectural patterns are used to ensure automatic failover and scaling.

Audit Logs

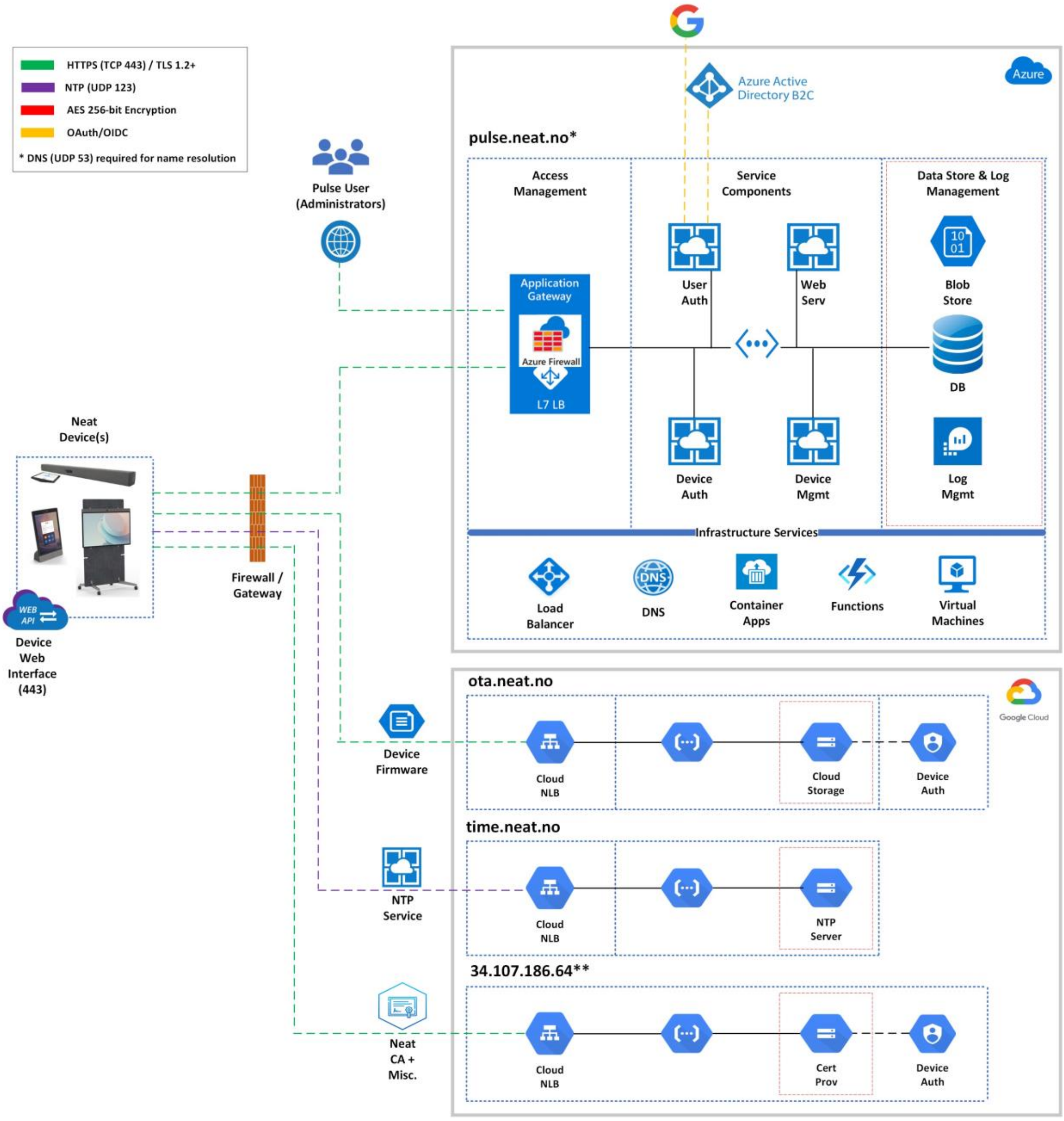
Neat Pulse allows Customers to export audit logs which contain user action logs and device change logs. Both user action logs and device change logs may include personal data such as first name, last name, and email address. Audit logs are available for inspection and download for customers on the appropriate plan. The audit log retention period is 90 days.

Managed Services

Pulse makes heavy use of Microsoft Azure, ensuring underlying systems are managed and up to date. This means application and operating system patches are managed automatically by Azure. When new components are created, they are designed to make use of such managed services, minimizing the operational complexity and therefore increasing the overall security of the system.

High-Level Architecture

The following diagram is a logical representation of the Pulse services hosted in Microsoft Azure as well as services that devices rely upon, hosted in Google Cloud Platform. The diagram provides a high-level overview of the communication protocols in use, access management controls, services components, and storage architecture to run Pulse.



Reference: https://support.neat.no/article/network-and-firewall-requirements-for-neat/

*pulse.neat.no IP addresses:
20.76.42.235 | tcp 443
20.16.158.114 | tcp 443
108.142.134.73 | tcp 443
13.81.211.248 | tcp 443

**Neat uses the same static IP address (34.107.186.64) for all the HTTP and HTTPS services below:
connectivitycheck.neat.no | 34.107.186.64 | tcp 80 (http) and tcp 443 (https)
id.neat.no | 34.107.186.64 | tcp 443 (https)
api.neat.no | 34.107.186.64 | tcp 443 (https)
metrics.neat.no | 34.107.186.64 | tcp 443 (https)

Secure Development Lifecycle

Security and Privacy by Design

The Pulse architecture is designed to minimize data sharing. Each organization or tenant's data is stored in its own independent database. Architectural decisions follow a collaborative design process, security and privacy review, and require sign-off by the senior level of engineering before implementation.

Software Development

Software is developed using the modern collaboration features of GitHub. Source code is stored on GitHub, guaranteeing change history, availability, and resilience of the assets. Changes are peer reviewed before being merged into a release, and changes are accompanied by unit and integration tests suitable for the feature or fix. Tests are run on every change (continuous integration) and software releases are only produced if all tests pass. Every successfully tested build automatically results in a new release (continuous delivery), which can be deployed to production quickly and easily.

Change & Release Management

The Pulse system is carefully designed to minimize changes such that a new version of software can be deployed incrementally to users and customers, rather than all at once. This allows a carefully staged software release, and also cutting-edge features to be tested by beta testers, without affecting the majority of users. Changes to the production system follow a DevOps paradigm of using software development processes and principles: peer code review, change history, and infrastructure as code.

Security Scanning

Automated software dependency scanning is used to detect potentially vulnerable software package dependencies. SAST tools are used to automatically scan and automate some of the update procedures. The Neat Pulse operations team also performs routine scans that are used to inspect the Microsoft Azure installations of Pulse for security best practices. We routinely engage independent third-party security firms to conduct penetration testing across our services. These assessments are designed to identify and remediate potential vulnerabilities, strengthen our security posture, and validate the effectiveness of our controls.

Pulse API Rate Limits

The Pulse API has rate limits in place to ensure that load and request traffic is being handled efficiently. The rate limit defines the maximum number of requests that can be made to the API within a given period of time. The default maximum rate limit is 10 requests per enrolled device per 5 minutes, calculated per Pulse organization. In addition, the API is rate limited to a maximum of 15 requests/second, calculated per integration token. If the rate limit is exceeded, the API request will fail and return a HTTP 429 status code.

Error handling best practices:

- Use bulk endpoints when fetching sensor data
- Reduce request frequency where possible
- Implement a wait before retrying
- Run requests sequentially rather than in parallel
- Note that rate limits may be subject to change.

Remote Control

The Pulse Remote Control is a feature allowing full remote access to a Neat Device from the Pulse web portal. The power of this is accompanied by a thorough set of privacy controls. Any remote-control session allows both visibility of the remote control being active, and ability to refuse the start of the session.

Devices maintain a configuration setting that is not managed by Pulse: whether to Allow, or Not Allow remote control requests.

When remote control is requested from Pulse:

- If the setting is Not Allowed, then the remote control will not proceed.
- If the setting is Allow, a time-limited dialogue is shown allowing a user to cancel the request. If the user chooses to disallow, the remote-control session will not proceed.

If the remote-control session does proceed with the required consent / configuration, then information that the session is active is shown on the device or devices being remote controlled. The remote-control session can be ended on the endpoint at any time.

Remote control sessions are audited to the audit log. The remote-control feature can be disabled from the endpoint, you can only re-enable control again from the endpoint. In the event a device is factory reset, the device then needs to be re-enrolled into Pulse. By default, remote-control is enabled after enrolling in Pulse. Please visit the neat support site (https://support.neat.no) for more information on remote-control features.

Data Privacy

Refer to the *Neat Data Processing Addendum (DPA)* for details regarding the processing of personal data that is subject to Data Protection Laws in the scope of Neat Pulse ("Services").

Data Residency

Neat leverages third-party cloud hosting providers to deliver Pulse services globally. The cloud hosting providers are currently located in the following countries listed in *Table A*; however, locations may change over time. This document will be updated to reflect those changes in the event they occur. Note, that the cloud hosting providers listed below are specific to Neat Pulse services and do not reflect hosting locations for any applications or services running on a Neat device(s). All user authentication data is maintained by the Microsoft Azure B2C database, which provides a singular global view of users needed to allow login and authorization.

Table A

Cloud Hosting Provider Name	Location
Microsoft Corporation	Netherlands (Azure West Europe)

Certifications

Neatframe Limited and its subsidiaries are ISO/IEC 27001:2022 certified. The scope of this certification encompasses the processes, systems, and services responsible for the development, management, operation, sales, marketing, and delivery of Neat's products. This certification reflects Neat's commitment to maintaining a robust Information Security Management System (ISMS) aligned with internationally recognized standards.

Documentation

Software architecture, procedures and policies are stored on a central collaboration hub. This service allows instant collaboration, is backed up, and keeps a change history.

Information Security Incident Management

Neat maintains a Security Incident Response plan which outlines the general steps for responding to computer security incidents impacting Neat products as well as the operational aspects of Neat's internal information systems. The plan identifies incident response stakeholders and establishes their roles and responsibilities; describes incident triggering sources, incident types, and incident severity levels. The plan also includes requirements for testing, post-incident lessons-learned activities, and the collection of metrics to use in gauging response effectiveness.

There may be circumstances where Neat will contact customer(s) in the event of a data breach that could impact sensitive data. Neat does not collect, store or transfer sensitive customer information; however, performing normal business operations typically includes some level of Personally Identifiable Information (PII) - this may include email address, first and last name. Neat will promptly notify customers of any actual or alleged incident of unauthorized or accidental disclosure of or access to any personal data or other breach.

Customers can also report a security concern regarding a Neat device(s), by visiting https://support.neat.no/ or contacting us at support@neat.no.

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 Pulse service, please email: support@neat.no and one of our technical support engineers will reach out to you.

Disclaimer

This document is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Neat product. You may copy and use this document for your internal reference purposes only. All statements, information and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. This document is not an agreement and in no event will Neat be liable for lost profits or loss of business or for any consequential, indirect, special, incidental or punitive damages arising out of or related to this document. The specifications and information regarding the products and/or services in this document are subject to change without notice.