\Orchestrating a brighter world NEC

UNIVERGE BLUE®
MEET

Security Guide

UNIVERGE BLUE®
MEET

NEC invests considerable human and capital resources to help ensure a secure UNIVERGE BLUE® MEET experience for our customers. Through the use of numerous security features built into the product, regular security audits by third parties and continued investment in our security environment, NEC makes every effort to deliver a highly secure service that protects the confidentiality of the participant data and meeting content with which we are entrusted by users of our service.

IN THIS GUIDE, YOU WILL LEARN HOW NEC HELPS ENSURE THAT YOUR UNIVERGE BLUE® MEET EXPERIENCE IS ALWAYS SECURE:

- What security features we offer to keep you safe from unwanted participants and hackers
- How we keep the NEC network secure for UNIVERGE BLUE® MEET
- Which industry and compliance standards we adhere to
- How NEC keeps your data private and secure

WHAT SECURITY FEATURES KEEP UNIVERGE BLUE® MEET USERS SAFE FROM HACKERS AND UNWANTED PARTICIPANTS?

FEATURES THAT STOP UNWANTED PARTICIPANTS

Can others join my online meetings before I do?
No. The UNIVERGE BLUE® MEET account holder is always required to start the online meeting first; any early arrivals will not be able to view content or interact with any other invitees via the online meeting until that happens. They will simply see a screen showing that the meeting isn't yet started.

Can I lock my meetings?
Absolutely. Once a meeting has started, the host has the ability to LOCK the meeting. The meeting lock feature ensures that no one else can join a meeting, potentially snooping in or disrupting the session. To enable this feature for a meeting, simply press the on-screen lock button once all attendees are present in the meeting.

How do I make sure people can't crash my meetings?
When scheduling your meetings through UNIVERGE BLUE® MEET's Meeting Dashboard, UNIVERGE BLUE® MEET generates a random meeting code, which is part of the unique link required to attend the individually scheduled meeting. This code prevents anyone from attending if they do not possess the meeting code.

How can I make sure people don't crash my conference calls?
While meeting codes provide a unique link for the online meeting attendees, an attendee dialing in on the phone would also need to know the unique meeting PIN in order to gain access to the meeting. To set up meetings with unique meeting PINs, make sure you're scheduling your secure meetings through UNIVERGE BLUE® MEET's Meeting Dashboard.

Can I remove unwanted attendees?
UNIVERGE BLUE® MEET hosts may mute or expel participants at any time during the meeting with a single click. Simply click on the attendee in the Attendee List and select "Remove from Meeting."

HOW UNIVERGE BLUE® MEET KEEPS DATA SECURE

Are meetings encrypted?
UNIVERGE BLUE® MEET establishes a connection between the user's client (browser, desktop app or mobile apps) and our web server using Secure Sockets Layer (SSL) signaling. This is an industry-standard encryption technology that helps ensure that connection details passed on the network remain private. Audio and video information transported over the Internet uses WebRTC encryption standards such as Datagram Transport Layer Security (DTLS), which prevents eavesdropping or tampering, and Secure Real-time/ Control Transport Protocol (SRTP and SCTP), which provides authentication and data integrity while in-transit. However, please note that participants who join our online meetings via traditional dial-in PSTN (landlines or cellphones) transmit their meeting audio unencrypted. Those calls are not made through NEC's secure apps, so they have the same level of security that applies to all cellular or land-line phone calls.

Are my meetings recorded automatically?
No. Meetings are NOT recorded automatically. In order to record a meeting, the meeting host must manually initiate it by pressing an on-screen "record button." By default, all participants in a meeting are alerted when the meeting is being recorded.

Who can access my recordings?
Once the meeting has concluded, the meeting host initially has sole access to the meeting recording. From that point, they may then download the recording, share the file, or send out a link to the recording.

Meeting recordings can be password protected through our administrator screens, which are controlled by the hosts of each individual meeting. The host may do this as shown in our KB article.

Meeting recordings are retained until they are deleted by the host using the administrator tool, at which point the recording is completely deleted from NEC's servers. NEC suggests that administrators create a policy with their employees as to how recordings are managed as a company.

How are my recordings protected?
Meeting recordings are stored in highly secured storage using AES-256 encryption, in North American availability zones. Meeting recording links can optionally be secured using a strong password. Finally, recordings can be configured to require a name and email from every viewer, giving the host a report of who's watched the recording.

Can anyone spy on my audio, video or shared screens?
UNIVERGE BLUE® MEET uses DTLS and SRTP security protocols with strong encryption to keep audio and video from being accessed by a "man-in-the-middle" attack, where network traffic could be snooped while in transit. In addition, we enable meeting hosts to stop unwanted participants from gaining access to your meetings through random meeting codes for scheduled meetings, attendee PINs, and meeting lock.
See this article for more information.

How secure is the In-Meeting Chat? How about the Notes?
Meeting notes and chat are encrypted in transit using SSL, so they cannot be seen by anyone other than people attending your meetings. Meeting records of chat and notes are stored on our highly secured servers, in our encrypted databases.

Who can see who attended my meeting?
After a meeting has concluded, only the host of the meeting has the record of the attendees, which can be found in the "My Meetings" section of the user's secure account page.

What countries does my meeting data travel through?
UNIVERGE BLUE® MEET servers are located in tier-three datacenters at various locations throughout the United States and the United Kingdom. As we expand capacity to other regions, we will use highly secure infrastructure from AWS or other reputable providers.

Does UNIVERGE BLUE® MEET offer End-to-End Encryption?
End-to-end encryption means that all data and traffic is encrypted and can only be decrypted by the attendees of a specific call or meeting, and that servers in the middle of those calls cannot access any of the call data.

UNIVERGE BLUE® MEET encrypts all traffic between meeting attendees and our servers. However, NEC must be able to decrypt this traffic, in order to deliver all of the rich features of our service, such as recording, audio conferencing mixing and meeting transcripts. This is consistent with current industry standards.

In addition, participants who join meetings via dial-in PSTN listen to the meeting audio unencrypted. Those calls are not made through NEC's network, so they have the same level of security that applies to all cellular or land-line phone calls.

As a result, UNIVERGE BLUE® MEET does not claim to offer "end-to-end" encryption. However, our service provides high levels of security and privacy, consistent with industry standards, for all of your business meetings.

What is the Virtual Assistant and is it secure?
The Virtual Assistant is a feature that captures your meeting audio and transcribes it for you so that you don't miss any details in your meetings. It also provides Meeting Insights, which are delivered in the form of a list of tasks.

Only the host receives a meeting transcription overview, sent to the email address that is associated with the UNIVERGE BLUE® MEET account. It includes a secure link to review your complete transcript and Meeting Insights, which are stored in your Account page. This feature uses 2048-bit AES encrypted connections to Google Cloud's speech-to-text platform (which meets numerous compliance and regulatory assurance) and anonymously converts the meeting audio to text.

WHAT INDUSTRY STANDARDS DOES UNIVERGE BLUE® MEET ADHERE TO?

SOC 2 Type 2

SOC 2 is a technical audit standard specifically designed for service providers who store and process customer data in the cloud. NEC regularly obtains a SOC 2 report from an independent auditor who validates that, in their opinion, NEC's controls and processes are effective in minimizing risk and exposure to this data.

HIPAA

UNIVERGE BLUE® MEET enables HIPAA compliance for its customers and its partners. When paired with well-defined security and privacy controls that are the responsibility of the customer, UNIVERGE BLUE® MEET enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) to use NEC's secure environment to process, maintain, and store protected health information (PHI).

"HIPAA compliance" requires that a service can be used in a way that protects PHI and is covered by a Business Associate Agreement (BAA) between the service provider (in this case, NEC) and either the healthcare provider (which is classified as a "covered entity" under HIPAA) or a business associate of the covered entity (such as an IT provider that resells NEC services to the covered entity). UNIVERGE BLUE® MEET meets these requirements based on administrative, physical, and technical controls to safeguard the confidentiality, integrity, and availability of PHI, and NEC will provide a BAA covering the UNIVERGE BLUE® MEET service to any customer or partner upon request.

GDPR

This European privacy regulation governs the processing and handling of personal data relating to individuals in the European Union. NEC handles all personal data in compliance with GDPR. A GDPR-compliant Data Processing Addendum that covers our products, including UNIVERGE BLUE® MEET is included in our service agreement.

PCI DSS 2.0

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. The payment processing system utilized by NEC undergoes regular testing and is compliant with the PCI DSS requirements. This helps ensure that your payment information will not be accessed by unauthorized parties or shared with unscrupulous vendors.

CPNI

Consumers are understandably concerned about the security of the sensitive, personal data they provide to their service providers. The Federal Communications Commission (FCC) requires carriers like NEC to establish and maintain systems designed to ensure that we protect our subscribers' Customer Proprietary Network Information (CPNI). Each year, NEC files an annual certification documenting our compliance with these rules.

CCPA

The California Consumer Protection Act (CCPA) went into effect on January 1, 2020. This new law allows any California consumer to demand to see all the information that a company possesses about them, as well as a full list of any third parties that the data is shared with. NEC is compliant with this California state law and does not sell your personally identifiable information.

HOW DOES NEC ENSURE THAT YOUR DATA IS PRIVATE AND PROTECTED?

How we treat personally identifiable data

NEC offers a clearly documented Privacy Policy, which governs our treatment and handling of sensitive data, including personally identifiable information.

NEC also adheres to the EU-U.S. Privacy Shield Framework set forth by the U.S. Department of Commerce and the European Commission.

To read NEC's complete Privacy Policy, please visit this link.

Employee security

NEC employees undergo rigorous background checks. Employee access to passwords, encryption keys and electronic credentials is strictly controlled using two factor authentication and role-based access control. Access to servers is restricted to a limited number of authorized engineers and monitored regularly.

Authentication and access

NEC has established a number of stringent policies and procedures to authenticate a caller's identity during support and service calls. These policies and procedures help protect confidential information belonging to your account and to your users by helping to ensure that only authorized members of your team are given access to our services. In addition, our online control panel enables administrators to control access to services and administrative functions.

Dedicated security staff and monitoring

NEC employs dedicated, full-time security staff who are certified in information security. This team is involved with all aspects of security, including log and event monitoring, incident response, perimeter defense, endpoint detection and response, penetration testing, vulnerability management, architecture design, security awareness and source code reviews.

HOW IS UNIVERGE BLUE MEET INFRASTRUCTURE KEPT SECURE?

Active meetings are hosted and stored in geographically dispersed, highly secure and monitored datacenters within the United States and the UK, by certified reputable providers.

Each of NEC UNIVERGE BLUE's datacenters adheres to strict standards in physical security. Each datacenter is closely monitored and guarded 24/7/365 with sophisticated pan/ tilt closed-circuit TVs. Secure access is strictly enforced using the latest technology, including electronic security gates between lobby and datacenter, motion sensors and controlled ID key-cards. Security guards are stationed at the entrance to each site. NEC's UNIVERGE BLUE uses multiple redundant, enterprise-class firewall systems to help prevent unwarranted intrusions and to help ensure that only authorized users can access your cloud environment. This purpose-built security system integrates firewall, VPN and traffic management.

NEC UNIVERGE BLUE's also utilizes commercial and in-house systems to help detect and deter malicious network traffic and computer usage that often cannot be caught by a conventional firewall. The system monitors for unusual traffic patterns and alerts system administrators of any suspicious behavior.

Our systems can also help prevent network attacks against vulnerable services; data driven attacks on applications; host-based attacks such as privilege escalation; unauthorized logins and access to sensitive files; and malware (e.g., viruses, Trojan horses, and worms).

Other network security highlights:

- Commercial-grade edge routers are configured to resist IP-based network attacks
- Distributed Denial of Service (DDoS) protection is subscribed to through a leading provider of network security
- The production network is physically and logically separated with highly restricted access and multiple authentication levels
- Operational functions include monitoring, system hardening, and vulnerability scans

\Orchestrating a brighter world NEC

OVER
$26 BILLION
REVENUE

#1
SMB & ENTERPRISE COMMS WORLDWIDE

LEADER IN
BIOMETRICS

75 MILLION
GLOBAL USERS

TOP 100
GLOBAL INNOVATORS
(THOMSON REUTERS)

RECOGNIZED AS A LEADER
BY FROST & SULLIVAN IN ENTERPRISE COMMUNICATIONS TRANSFORMATION

125+
COUNTRIES

GLOBAL 100
MOST SUSTAINABLE COMPANIES IN THE WORLD
(CORPORATE KNIGHTS)

107,000
TEAM MEMBERS
WORLDWIDE

4,000+
CHANNEL PARTNERS

About NEC Corporation – NEC Corporation is a leader in the integration of IT and network technologies that benefit businesses and people around the world. By providing a combination of products and solutions that cross utilize the company's experience and global resources, NEC's advanced technologies meet the complex and ever-changing needs of its customers. NEC brings more than 120 years of expertise in technological innovation to empower people, businesses and society.

For further information please contact NEC Corporation of America or:

Americas (US, Canada, Latin America)
NEC Corporation of America
www.necam.com

EMEA (Europe, Middle East, Africa)
NEC Enterprise Solutions
www.nec-enterprise.com

Australia
NEC Australia Pty Ltd
au.nec.com

Asia Pacific
NEC Asia Pacific
www.nec.com.sg

Corporate Headquarters (Japan)
NEC Corporation
www.nec.com

SW20040 | v.06.19.20