BlueJeans by Verizon

BlueJeans by Verizon
System and Organization Controls ("SOC") for Service Organizations: Trust Services Principles Report Relevant to Security, Availability, and Confidentiality Related to the BlueJeans Cloud-Based Video Conferencing Services Platform

For the period September 1, 2022 to August 31, 2023

Standards for Attestation Engagements,
SOC 3® Engagement

bpm

Table of Contents

One California Street, Suite 2500, San Francisco, CA 94111
Phone 415-421-5757 | Fax 415-288-6288 | bpm@bpm.com

Section I – Independent Service Auditors' Report

To the Management
BlueJeans by Verizon
San Jose, California

Scope

We have examined BlueJeans by Verizon's ("BlueJeans" or the "Company") accompanying assertion titled "Assertion of the Management of BlueJeans" ("assertion") that the controls within BlueJeans' Cloud-Based Video Conferencing Services Platform (the "System") were effective throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

BlueJeans uses subservice organizations to provide certain aspects of the System, as follows:

- Data center hosting services
- Application hosting services
- Data storage services

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BlueJeans', to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria. The description presents BlueJeans' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BlueJeans' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BlueJeans, to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria. The description presents BlueJeans' controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of BlueJeans' controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

BlueJeans is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved. BlueJeans has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, BlueJeans is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the System.

Service Auditors' Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the System were effective throughout the period to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the System and BlueJeans' service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the System were effective to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination was not conducted for the purpose of evaluating or testing BlueJeans' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the System were effective throughout the period September 1, 2022 to August 31, 2023 to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Emphasis of Matter – BlueJeans Sunsetting

As noted in “Section III – BlueJeans’ Description of the System,” under paragraph “B7, Significant Events,” Verizon announced on August 16, 2023 that BlueJeans products and services will be retired in the first half of 2024. The free trial feature was discontinued as of August 31, 2023 and all new sales are stopped. All customers have been notified to migrate off the platform by February 29, 2024. BlueJeans Engineering, Operations, Support and Security personnel are currently working on a plan to shut down the products and services in an orderly manner by the end of June 2024.

Our opinion is not modified with respect to this matter.

San Francisco, California
November 21, 2023

Section II – Assertion of the Management of BlueJeans by Verizon

We are responsible for designing, implementing, operating, and maintaining effective controls within BlueJeans by Verizon's ("BlueJeans" or the "Company") Cloud-Based Video Conferencing Services Platform (the "System") throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that BlueJeans' service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the System (the "description") is presented in "Section III – BlueJeans' Description of the Boundaries of the System" and identifies the aspects of the System covered by our assertion.

BlueJeans uses subservice organizations ("subservice organizations") to certain aspects of the System, as follows:

- Data center hosting services
- Application hosting services
- Data storage services

The description indicates that complementary subservice organization controls ("CSOCs") that are suitably designed and operating effectively are necessary, along with controls at BlueJeans, to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls ("CUECs") that are suitably designed and operating effectively are necessary, along with controls at BlueJeans, to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria. The description includes the complementary user entity controls assumed in the design of BlueJeans' controls.

As noted in "Section III – BlueJeans' Description of the System," under paragraph "B7, Significant Events," Verizon announced on August 16, 2023 that BlueJeans products and services will be retired in the first half of 2024. The free trial feature was discontinued as of August 31, 2023 and all new sales are stopped. All customers have been notified to migrate off the platform by February 29, 2024. BlueJeans Engineering, Operations, Support and Security personnel are currently working on a plan to shut down the products and services in an orderly manner by the end of June 2024.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality ("applicable trust services criteria") set forth in TSP 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). BlueJeans' objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III E., Principal Service Commitments and System Requirements.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the period September 1, 2022 to August 31, 2023, to provide reasonable assurance that BlueJeans' service commitments and system requirements were achieved based on the applicable trust services criteria.

The Management of BlueJeans by Verizon

Section III – BlueJeans' Description of the Boundaries of the System

A. Company Overview

BlueJeans was founded in 2009 and is headquartered in San Jose, California, with offices in Dunedin, New Zealand, and Bengaluru, India. BlueJeans was acquired by Verizon Communications, Inc. (VZ) ("Verizon") and the acquisition closed on May 15, 2020. The integration with Verizon began in November 2020. Since then, as a subsidiary, the Company is known as BlueJeans by Verizon ("BlueJeans" or the "Company").

Data center hosting service providers are in the United States ("U.S."); the Netherlands; Singapore; and India. BlueJeans also uses Amazon Web Services ("AWS") (in the U.S., Singapore, Australia, India, and Ireland) and Microsoft Azure Cloud ("Azure") (in the U.S., Singapore, Australia, and the Netherlands). Details regarding BlueJeans' subservice organizations can be found in Section C. *Complementary Subservice Organization Controls ("CSOCs")*.

B. System Overview

1. Services Provided

BlueJeans provides a cloud-based video conferencing services platform (the "System") that allows individual users, teams, and groups to connect across many devices and platforms. With an integrated suite of video conferencing services (that includes Meetings, Events, and Rooms), BlueJeans offers companies, partners, and end users the power to expand phone calls into video calls. BlueJeans supports multi-party bridging, multi-vendor, and multi-device video calling. The BlueJeans feature set enables users to connect across several platforms (such as Polycom and Cisco) and endpoints (desktops, browsers, and smart devices, Android, and iOS). Each meeting can be secured and encrypted. Additionally, BlueJeans provides a gateway service which allows SIP (Session Initiation Protocol) and H.323 standards-based video conferencing room systems to join Microsoft Teams Meetings.

The video conferencing services provided include BlueJeans Meetings (core software), BlueJeans Events (broadcast), BlueJeans Rooms, Command Center (analytics), Relay (integration software for room systems and BlueJeans), the Administration portal, and Teams Gateway.

BlueJeans Meetings
Meetings seamlessly delivers interactive, two-way face-to-face video meetings that are secure and ready to scale from laptops, mobile devices, or room systems. The Meetings feature comprises integrated components that support a wide variety of room, browser, desktop, and mobile endpoints. It supports a range of telecommunication standards for audio-visual sessions and the call signaling helps transmit calls across the Internet Protocol ("IP") and Public Switched Telephone Networks. In addition, Meetings supports H.323 and Session Initiation Protocol ("SIP") for controlling audio-visual sessions over IP networks.

BlueJeans Events
Events blends the interactivity and engagement of a video meeting with the scalability of a broadcast event, by creating an easy, open, and collaborative experience for both organizers and attendees.

BlueJeans Rooms
Rooms provides the capability to make any conference room an easy-to-use video room that interoperates with existing systems or new hardware.

Relay
Relay is a software platform that integrates user entity-premise components and applications with the BlueJeans cloud for a collaboration experience. Relay Touch integrates calendar applications, conference room systems, and tablet devices to make joining a BlueJeans meeting easy and automatic.

Command Center
Command Center is an analytics dashboard for user entities and provides insights into historical meetings, events, and room's usage and related information.

The Administration Portal
The Administration portal is used by Enterprise Administrators for managing users and organization-wide policies in BlueJeans System.

Teams Gateway
Teams Gateway is a cloud service which enables standards-based (SIP and H.323) video conferencing room systems to join Microsoft Teams Meetings. The service is hosted in Azure.

2. Infrastructure

BlueJeans' services are hosted in multiple tier-4, secure co-location data centers around the world. BlueJeans hosts the application layer with database infrastructure in two regions (us-west-2 and us-east-1) in AWS. The media infrastructure is hosted in four Equinix, Inc. ("Equinix") data centers (in the U.S.; Amsterdam, the Netherlands; and Singapore), four Verizon data centers (Sacramento, Twinsburg, Singapore and Amsterdam), one Nxtra Data Ltd ("Nxtra") data center (in India) and several AWS regions around the world including Ireland (eu-west-1), Australia (ap-southeast-2), Singapore (ap-southeast-1), India (ap-south-1), and the U.S. (us-west-1, us-west-2, us-east-1, and us-east-2). See Section *C. Complementary Subservice Organization Controls ("CSOCs")* for additional information.

The production environment and the development environment utilize physically separate network, data, and server infrastructures. Access to the cages in the co-location data centers is restricted to authorized BlueJeans Operations personnel. The ability to deploy code to the production environment is restricted to authorized Operations Team members.

BlueJeans hosts the Teams Gateway on Azure in four regions: the U.S. (West-US), the Netherlands (West-Europe), Australia (New South Wales), and Singapore (APAC).

3. Software

BlueJeans' video conferencing services platform (the "Platform") is built on Linux. Teams Gateway uses both Linux and Microsoft Windows. BlueJeans' client service products include desktop clients on Mac, Windows, and Linux; mobile clients on iOS and Android; and web clients on Chrome, Safari, Firefox, and Internet Explorer browsers. Additionally, Room system clients are supported. Calendar integrations with Microsoft Exchange, Microsoft Office 365 and Google Calendar are supported.

BlueJeans leverages industry standard third-party software tools to support the Platform. Only authorized Engineering personnel have access to the source code repository. All software releases are version controlled. The software release process incorporates architecture and security reviews, peer reviews of code and quality gates as mandatory steps, which strengthen the quality of deliverables.

Section III – BlueJeans' Description of the Boundaries of the System

BlueJeans utilizes several monitoring frameworks for tracking security, performance, and effectiveness of systems, and applications used to support the Platform. Alerts are configured to notify Engineering, Operations and Security personnel when components of the Platform operate outside acceptable thresholds. Alerts related to security, availability, and confidentiality incidents are triaged, addressed, and remediated to meet service commitments.

4. People

BlueJeans' leadership and organizational structure provide a framework for planning, executing, and controlling business operations. Starting with the Executive Management Team that reports to Verizon's top management, this structure provides the leadership and vision to help ensure success of the System services, adequate staffing, security, efficiency of operations, and segregation of duties while setting the tone and establishing the core values of BlueJeans.

BlueJeans follows a structured on-boarding process to familiarize new employees and contractors with BlueJeans applications, processes, systems, security policies and practices. New hires are provided with the BlueJeans' Code of Conduct and are required to complete an initial and an annual Security and Awareness training. BlueJeans maintains high standards for hiring and places emphasis on education, integrity, and functional roles performed previously to assess if a candidate is a "good fit" for the team. BlueJeans has also implemented controls over the key aspects of the off-boarding process. When the need arises for termination or separation, Human Resources ("HR") maintains an exit checklist and initiates/approves their termination.

The Executive Management Team has regularly scheduled meetings to discuss business strategy (including user entity challenges and legal updates), development, releases and enhancements to the product line and other important matters. In addition, the Executive Management Team develops a summary of recent business activity and presents it at regularly scheduled (usually quarterly) and special meetings to Verizon Business Group ("VBG") leadership.

The Operations Team along with the Information Security Team designs key controls and monitors the operation of those controls to meet service commitment efforts for BlueJeans. The Chief Technical Officer ("CTO") and the Deputy Chief Information Security Officer ("Deputy CISO") delegate responsibility for internal information technology ("IT") related controls to other members of the organization where needed. To maintain these standards and help ensure that employees understand and follow internal policies, certain control activities are performed.

To help secure the System and the business operational environment, management has documented and implemented policies. These policies and standards documents are reviewed, managed, and updated (annually) by the CTO or the Deputy CISO to help ensure security and confidentiality measures and availability concerns are addressed.

5. Data

BlueJeans collects minimal personal data from user entities for authentication and personalization when using the video conferencing service. When the user entity participates in a meeting, the call detail records are collected and stored for reporting and analytics purposes. Each Enterprise's data is logically separated from others in the database using a unique ID. BlueJeans encrypts data at rest using AES-256. Data in transit protections include using Transport Layer Security ("TLS") for web traffic and Secure Real Time Protocol for media traffic using AES-128 at a minimum. User access to production data is based on their role after authentication. Within BlueJeans, access to protected systems and data are granted to employees based on their role, the business need-to-know and the principle of least privilege. When an employee leaves BlueJeans, the user termination process revokes the logical access within one (1) business day of termination date. The access list is reviewed quarterly by the Deputy CISO or delegate and any unnecessary permissions are removed.

When a user entity records a meeting, the user entity is responsible for the content. The recording is stored encrypted in AWS S3 using AES-256. The user entity owns the recording by default. BlueJeans provides storage and a permissions framework for managing the recording.

BlueJeans has documented policies for decommissioning production equipment that no longer meets the service objectives and destroys any media containing data and software physically using a third-party vendor on site.

6. Processes and Procedures

Access to the System

BlueJeans deploys firewalls, system-hardening procedures, standard application and secure protocols for access, and third-party monitoring to protect against unauthorized access to systems.

BlueJeans restricts access to the production environment to only those employees with a job function that requires access using two factor authentication ("2FA") over a virtual private network ("VPN").

User entities access BlueJeans administrative applications through web interfaces using their role. User entities can manage only their profile data, schedule and host meetings, and view reports (when such permissions are granted to them). Administrators can manage other users, set policies, and view reports.

Administration of the System

BlueJeans' Operations Team is responsible for performing all operational tasks per approved policies and procedures, including tracked change/patch management for updating application binaries, data, software stack, hardware, and emergency fixes, monitoring the System for performance, capacity, and availability, and maintaining backups of production data.

Core Security, Protection, and Confidentiality

BlueJeans documents its overall security approach in its Information Security and Confidentiality Policy document. Within this document are key areas describing how BlueJeans addresses the classification, protection, handling, responsibility, transmission, storage, and access of data.

To protect confidential data, the control framework that underpins the BlueJeans organizational environment starts with the Executive Management Team and is executed by their respective managers and teams. BlueJeans communicates its confidentiality commitment to every user entity within the contract prior to delivery of the service. Appropriate logical security controls are implemented by IT to help ensure that System access is restricted to employees with a business need-to-know and System access is monitored.

The System is designed to enable authenticated user entities to access and manage their recorded and/or uploaded video content and manage access to the System. BlueJeans has also implemented technical and physical controls designed to prevent unauthorized access to or disclosure of content. Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting user entities' content. BlueJeans monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments. See Section C. Complementary Subservice Organization Controls ("CSOCs") below.

Section III – BlueJeans' Description of the Boundaries of the System

Overall, management's philosophy, its skilled managers and the underlying culture contribute to the strength of the control environment. This philosophy influences how user entities are supported, how internal decisions are made, and how risks are addressed.

Risk Management

BlueJeans Risk Management Methodology includes: i) identifying and categorizing assets into different classes, ii) working with functional heads of departments to calculate risk impact rating of assets based on the assets' value, threats and vulnerabilities to those assets, and the probability of occurrence of such threats and iii) implementing a risk treatment plan to mitigate high risks.

The Deputy CISO or designee maintains the identified risks in a "Risk Register." The risks are categorized by functional areas with identified risk owners. The list is reviewed at least once annually with individual stakeholders to remove risks that no longer apply, add new entries, or update existing entries. Newly identified risks are reviewed and tracked by management and a decision is taken to create mitigating controls or accept the risk presented to BlueJeans. Finally, the CTO or designee reviews and approves the risk register.

BlueJeans proactively identifies fraudulent use of the System by analyzing the repeated login and meeting join failures using Fraud Detection Service ("FDS"). BlueJeans' Support Team reaches out to impacted user entities to address the issue by changing password complexity or meeting settings, as necessary.

Incident Management and Communication

BlueJeans strives to provide a robust communication process to its user entities, vendors, and employees. The Executive Management Team is committed to maintaining an effective communications system to ensure System related issues, outages, and critical fixes are addressed and resolved in accordance with Service Level Agreements ("SLAs").

Incident Management procedures are triggered if there is severe degradation, an outage of the System, a suspected breach, or a known intrusion. All incidents are logged into the issue tracking software and tracked through to completion by the Engineering, Security, Support, IT, or Operations team. The Executive Management Team is informed of the incident management progress. If the production environments are inaccessible for any significant period, Customer Support will communicate the status via https://status.bluejeans.com and provide periodic updates when the System is being restored.

BlueJeans has a designated senior management contact within Customer Support to establish and maintain communication mechanisms that help ensure all user entities are provided new release information and any user entity issues are addressed and resolved to the user entity's satisfaction.

Product Planning, Release Cycle and Testing

To meet the needs of user entities, BlueJeans attempts to have manageable release cycles that are short in duration, predictable in delivery and flexible to meet a variety of needs. BlueJeans follows a documented "Software Release Process" that includes steps for the product releases, emergency fixes and configuration and infrastructure changes. The release methodology has segmented environments for development, Quality Assurance ("QA"), staging, and production. This segmentation allows BlueJeans to perform updates quickly, but not expose production to changes without proper testing and approval. All product releases and changes are tracked through the project tracking system. BlueJeans requires that only tested and approved changes shall be made to the System and all changes made are documented, tested and approved by the Change Approval Board ("CAB") and other stake holders prior to production rollout, except in emergencies when the changes are approved post-production rollout.

Policies and Procedures

BlueJeans has the following security policies, standards, and procedures in place (which are owned by the Deputy CISO) that are reviewed and updated annually.

- Acceptable Use policy
- Access Control policy
- Asset Management policy
- Backup Strategy
- BC-DR policy
- Cloud Security policy
- Data Backup standard
- Data Classification policy
- Data Retention policy
- Encryption Implementation
- Encryption policy
- Exception Handling policy
- Incident Management policy
- Log Management
- Media Destruction and Disposal procedure
- Risk Management procedure
- Security Procedures for IT Operations
- Supplier Management
- Information Security and Confidentiality policy
- Standard Admin Action Logging
- Standard Admin-Priv Access
- Standard Capacity Planning
- Standard Change Management
- Standard Password Management
- Standard Patch Management
- Standard Workstation Security
- User Provisioning procedure
- User Termination procedure
- Workstation and Teleworking policy

7. Significant Events

Verizon announced on August 16, 2023 that BlueJeans products and services will be retired in the first half of 2024. Free trial feature was discontinued as of August 31, 2023 and all new sales are stopped. All customers have been notified to migrate off the platform by February 29, 2024. BlueJeans Engineering, Operations, Support and Security personnel are currently working on a plan to shut down the products and services in an orderly manner by the end of June 2024.

C. Complementary Subservice Organization Controls ("CSOCs")

BlueJeans uses service organizations ("subservice organizations") to provide services related to the System.

The System's production data centers are located at Equinix data centers in the U.S., the Netherlands, and Singapore; a Nxtra data center in India; Verizon Data Centers in the U.S., Singapore, and Amsterdam; and several AWS regions around the world. The System is delivered from these facilities in geographically separate locations.

Aside from the main data centers helping to distribute the System, AWS services are used worldwide to augment the Company's data center capabilities.

Teams Gateway is hosted on Azure.

BlueJeans' controls were designed with the assumption that certain complementary subservice organization controls ("CSOCs") that are suitably designed and operating effectively would be necessary, along with controls at BlueJeans, to achieve BlueJeans' service commitments and system requirements based on the applicable trust services criteria.

Accordingly, the following table describes the types of CSOCs that are necessary at the subservice organizations used by BlueJeans:

Facilities Housing the System
CSOCs
Access to data and software is restricted to BlueJeans personnel authorized and provisioned with logical security controls.
Physical access to the facility housing the System is restricted to authorized personnel.
The entity identifies, selects, and develops risk mitigation activities for risks arising from potential disruption.
Environmental protections, software, data backup processes, and recovery infrastructure are operating, and monitored.
Disaster recovery procedures are tested at least annually.

The above-mentioned subservice organizations have provided a System and Organization Control ("SOC") for Service Organizations, SOC 2 Type II Report. BlueJeans requests such SOC reports and/or ISO 27001 certifications from the subservice organizations and reviews the reports for exceptions and complementary user entity controls ("CUECs") that must be implemented within the BlueJeans control environment.

D. Complementary User Entity Controls ("CUECs")

The System was designed with the assumption that certain CUECs are suitably designed and operating effectively, along with controls at BlueJeans, to achieve BlueJeans' service commitments and system requirements based on the trust services criteria relevant to security, availability, and confidentiality.

This section describes certain CUECs that should be operating effectively at user entities. However, there may be related controls not identified in this report that may be appropriate for a specific user entity's operation. Each user entity must evaluate its own internal control structure to determine if the identified controls are in place.

1. List of CUECs

CUECs
User entities are responsible for:
Ensuring the security and confidentiality of all user identifications ("IDs") and passwords, preventing unauthorized access to, or use of the System, and notifying BlueJeans Customer Support promptly of any actual or suspected unauthorized use of the System.
All activity under its user accounts, including notifying BlueJeans of failed login attempts from an unknown source.
Ensuring the confidentiality of any user accounts and passwords assigned to them for use with BlueJeans' systems, preventing unauthorized access to, or use of the System, and notifying BlueJeans Customer Support promptly of any actual or suspected unauthorized use of the System.
Disabling access of employees to the System immediately upon termination.
Ascertaining that expressed consent has been obtained from their users to transfer user data to the U.S., if applicable.
Identifying an administrative username and password for its account.
Accepting and complying with the Terms of Service with BlueJeans, in accordance with contractual agreements.
Following the contract guidelines regarding the System services.
Agreeing that the Service will be used only in compliance with BlueJeans' Acceptable Use Policy.
Understanding the operating systems, web browsers and mobile devices that can be used with the System and ensuring their security configurations are up to date.

CUECs
User entities are responsible for:
Reviewing the completeness and accuracy of the reports produced by the System.
Setting the proper configurations for each scheduled meeting based on the options provided by the System.
Communicating and providing up-to-date organizational contact information to BlueJeans.
Obtaining and maintaining any equipment or ancillary services needed to connect to, access or use of the System.
The accuracy, quality, integrity, legality, and appropriateness of the content.
Maintaining adequate backups of their content.
Determining the applicability of recording any parts of meetings.
Setting data retention of scheduled video conference meetings.
Notifying BlueJeans if they detect or suspect a security incident related to the System.

E. Principal Service Commitments and System Requirements

BlueJeans designs processes and procedures related to the System to meet its service objectives for its Cloud-based Video Conferencing services (the "services"). Those objectives are based on the service commitments that BlueJeans makes to user entities; relevant laws and regulations; and the financial, operational requirements that BlueJeans has established for the services.

Security, availability, and confidentiality service commitments and system requirements to user entities are documented and communicated in SLAs and other user entity agreements, as well as in the description of the service offering provided online. Security, availability, and confidentiality service commitments and system requirements include, but are not limited to, the:

- Use of encryption technologies to protect user entity data both at rest and in transit.
- Relevant physical and logical security controls designed to prevent unauthorized access to the infrastructure and service that support the System.
- Role-based security model to secure access to data hosted within the System.
- Corporate IT-related controls around endpoint protection and the security of data access environment.
- Use of continuous replication for databases and redundant data centers for high availability.
- Use of change management process to deploy only approved changes to the production infrastructure.

BlueJeans establishes operational requirements that support the achievement of security, availability, and confidentiality service commitments and system requirements; relevant laws and regulations; and other System requirements. Such requirements are communicated in BlueJeans' System policies and procedures, System design documentation, and contracts with user entities. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the System is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.