INTERMEDIA

The Business Cloud™

Intermedia.net, Inc.

Independent Service Auditor's SOC 3 Report

For the

Hosted Exchange and Intermedia Unite Systems

For the Period of July 1, 2019, to June 30, 2020

Attestation and Compliance Services

schellman

Quality, above all.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Intermedia.net, Inc.:

Scope

We have examined Intermedia.net, Inc.'s ("Intermedia") accompanying assertion titled "Assertion of Intermedia.net, Inc. Service Organization Management" ("assertion") that the controls within Intermedia's Hosted Exchange and Intermedia Unite (also referred to as "Unite") systems ("system") were effective throughout the period July 1, 2019, to June 30, 2020, to provide reasonable assurance that Intermedia's 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 section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Intermedia uses various subservice organizations for data center hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Intermedia, to achieve Intermedia's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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.

Service Organization's Responsibilities

Intermedia 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 Intermedia's service commitments and system requirements were achieved. Intermedia has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Intermedia is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's 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 the service organization's service commitments and systems 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 the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Intermedia's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Intermedia's 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.

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 Intermedia's 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 Intermedia's Hosted Exchange and Unite systems were effective throughout the period July 1, 2019, through June 30, 2020, to provide reasonable assurance that Intermedia's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHELLMAN & COMPANY, LLC

Tampa, Florida
September 11, 2020

Assertion of Intermedia Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Intermedia.net, Inc.'s ("Intermedia") Hosted Exchange and Unite systems ("system") throughout the period July 1, 2019, to June 30, 2020, to provide reasonable assurance that Intermedia's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2019, to June 30, 2020, to provide reasonable assurance that Intermedia's 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 section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Intermedia's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 July 1, 2019, to June 30, 2020, to provide reasonable assurance that Intermedia's service commitments and systems requirements were achieved based on the applicable trust services criteria.

Description of the Boundaries of the Hosted Exchange and Unite System

Company Background

Founded in 1995, Intermedia is a leading Unified Communications as a Service (UCaaS) and cloud business email and applications provider focused on delivering easy-to-use and secure communication and collaboration solutions to businesses and the partners that serve them. More than 125,000 business customers and 6,600 active partners rely on Intermedia's tightly integrated suite of cloud applications that are managed through one intuitive point of control and are backed by 99.999% uptime service level agreements (SLAs) and J.D. Power-certified 24/7 technical support. Solutions include the all-in-one cloud communication and collaboration platform - Intermedia Unite®, web and video conferencing, file sharing & backup, business email, security, archiving, and more.

The privately held company is headquartered in Sunnyvale, California, with additional offices in New York City, New York; Bellevue, Washington; Irvine, California; Bristol, United Kingdom; and St. Petersburg, Russia.

Description of Services Provided

Intermedia provides SMBs and the channel partners that serve them with the business cloud applications, service and support that make them more collaborative and productive.

Intermedia's offerings include:

- **Intermedia Unite®:** a fully integrated unified communications (UC) and collaboration platform for SMBs that combines a Cloud Private Branch Exchange (PBX) phone system with web and video conferencing, team chat, file sharing and backup, and much more.
- **Cloud PBX:** a business-class PBX offering that creates an integrated experience for Microsoft Exchange or Office 365® users by enabling features like click-to-call under one integrated platform. Additional Voice Services include session initiation protocol (SIP) trunking, conference calling, toll-free numbers, and internet fax.
- **Intermedia SecuriSync® Backup and File Sharing:** a business-grade, all-in-one file management service, which lets users back up files and folders, as well as share and sync files both internally and externally using virtually any device. Integrated Bitdefender anti-malware and anti-virus software provides an additional layer of protection.
- **Intermedia AnyMeeting®:** a video conferencing, web conferencing, webinar, screen sharing and conference call service that enables users to participate in highly interactive and productive meetings with participants in multiple locations. The service integrates with over 400 third-party applications.
- **HostPilot® Control Panel:** Intermedia's proprietary cloud management portal, which offers a single point of control for customers, partners, and end users. It allows partners and customers to easily add new services, manage app settings, respond to user service requests, get reports and much more. For partners, it also allows them to white-label their services, manage customers' services, and control billing. HostPilot is also available via mobile app for administrators, channel partners and end users.
- **Intermedia's Exchange E-mail:** based on Microsoft Exchange Server and comes with unlimited storage per user. Intermedia offers Exchange in shared or Private Cloud deployments. Intermedia's e-mail service integrates with other Microsoft platforms including Skype® for Business and SharePoint®.
- **E-mail Archiving:** provides preservation, protection and recovery features that meet or exceed compliance requirements. Provides unlimited, tamper-proof archiving of Exchange or Office 365 e-mails sent and received, helping with eDiscovery and safeguarding intellectual property.
- **Intermedia E-mail Protection:** anti-spam and anti-virus filtering included with every Exchange E-mail mailbox. Uses multiple e-mail security engines to provide protection against known, unknown, and emerging e-mail threats, over and above what single engine services can offer. It also includes LinkSafe™, which prevents users from clicking and accessing known phishing sites or webpages.

- **Policy & User-Based Encrypted E-mail:** allows users, based on their roles, to securely send confidential information over e-mail, allowing companies to better secure their e-mail communications.
- **Intermedia Office Apps Powered by Office 365**: extends the benefits of the Office productivity suite to Exchange e-mail users that choose not to use Office 365 for e-mail, by providing the latest desktop, mobile, and web versions of Microsoft Word, Excel®, PowerPoint®, Outlook®, OneNote®, Access and Publisher.

The scope of this report is restricted to Intermedia Unite (Intermedia Cloud PBX, SecuriSync, AnyMeeting), and Intermedia Hosted Exchange E-mail.

AnyMeeting, HostPilot, Intermedia Unite, LinkSafe, SecuriSync, and The Business Cloud are either registered trademarks or trademarks of Intermedia.net, Inc. in the United States and/or other countries. All other product names, trademarks and registered trademarks are property of their respective owners.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Intermedia has put into place a set of policies and procedures to help ensure that security, availability, and confidentiality commitments are met. Intermedia's commitments to user entities are documented in the master service agreement (MSA) for each customer, and Intermedia management has identified actions, in the form of control activities, to enforce those standards. Control activities are a part of the process by which Intermedia manages risk to achieve its business objectives. Intermedia makes the following security and availability commitments to its customers:

- Maintain security procedures that are consistent with applicable industry standards
- Establish escalation procedures with customers
- Ensure that security controls that meet customers' standards will be maintained to the level as attested
- Intermedia commits to providing the systems with a 99.999% uptime service level agreement

Intermedia communicates its SLAs through its MSA with customers during the contractual agreement process. The SLAs/MSAs are specific to services purchased by the customer, and these documents outline availability, warranty, maintenance schedules, and emergency maintenance schedules along with remedies. Per Intermedia's MSA, customers are responsible for securing necessary data from the account prior to contract termination. In addition, customers' data will be deleted promptly (as soon as fourteen calendar days) following the termination of the subscription for the applicable service.

System requirements are communicated in Intermedia's policies and procedures, system design documentation, and its SLAs through its MSAs with customers during the contractual agreement process. 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, trained, and managed. 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 breach protection services system.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Intermedia's production environment is hosted at third-party data center facilities. The third-party data center hosting providers are responsible for physical access management and environmental protection for production systems hosted at the facilities.

Intermedia's network is segregated into two primary domains: Corporate and production domains. The Corporate domain is used for internal systems and applications, and the production domain is used to manage and administer production user accounts, servers, applications, and systems. Employees can log in to Intermedia's systems using an encrypted virtual private network (VPN). VPNs are configured with security controls that enforce two-factor authentication, requiring individual username, personal identification number (PIN), and passcode for user authentication. Intermedia uses transport layer security (TLS) security protocols for transmitting data over unsecure networks.

Intermedia is architected in a virtualized environment supported by industry standard hardware. Intermedia Unite (SecuriSync, AnyMeeting, and Cloud PBX), Hosted Exchange, and the HostPilot control panel are deployed primarily on servers running industry standard operating systems and database engines. Access to the in-scope applications is managed through the HostPilot control panel.

Firewalls are in place and configured to Intermedia standards to prevent unauthorized communications. Network based intrusion detection systems are configured to detect attacks or suspicious behavior, and vulnerability scans are performed to identify potential weakness to the security and confidentiality of systems and data. System and network security is important to Intermedia and its customers. In order to maintain a secure infrastructure, Intermedia has several layers of security controls in operation. These controls include processes for managing user access to systems and devices, formal policies for authentication and password controls, and configuration standards for firewalls. Intermedia has implemented several monitoring controls to identify potential security threats and notify its personnel of the severity of the threat. Firewalls are in place and configured to Intermedia standards to prevent unauthorized communications. Network based intrusion detection systems are configured to detect attacks or suspicious behavior, and vulnerability scans are performed to identify potential weakness to the security and confidentiality of systems and data.

Intermedia utilizes commercial and proprietary security tooling to assist with threat and vulnerability management; security information event management; identity, access and passwords audits; secrets and key management; managed detection and response; security development lifecycle; managed security operations and managed penetration testing.

People

Intermedia has a defined organizational structure that includes the core functions supporting the in-scope systems. Personnel involved in the operation and use of the system are:

- **Intermedia's Management Team** – responsible for establishing information technology (IT) policies, standards, procedures, and guidelines covering access, security, privacy, confidentiality, and enforcement of procedures across the organization. Intermedia ensures that policies and procedures are reviewed annually and are updated on an as needed basis to reflect changes in the operating environment. The most current versions of the policies and procedures are posted on the intranet and are made available to employees for their review.
- **IT Operations** – responsible for management and operations of systems and networks.
- **Information Security and Privacy** – responsible for managing and maintaining various security and privacy policies, performs risk assessments, and performs monitoring to detect attack attempts.
- **Internal IT Support** – responsible for end-user workstation security, e-mail security, and Corporate systems supporting in-scope systems.
- **Core System Administration (CSA)** – responsible for management and administration of core systems.
- **Production System Administration (PSA)** – responsible for management and administration of production systems.

- **Network Engineering Voice Services** – responsible for management and administration of Cloud Voice production systems.
- **The Network Engineering and Data Center Operations Teams** – responsible for maintaining the safety and security of the buildings that house the in-scope systems.
- **Technical Support (Level 1 (L1), Level 2 (L2) and Level 3 (L3))** – responsible for resolving customer problems and inquiries.
- **Customer Support** – responsible for resolving customer problems and inquiries.
- **Technical and System Development Teams** – responsible for Development, Quality Assurance and Release Management activities.
- **The Quality Assurance and Release Management Teams** – responsible for reviewing releases for compliance with standards and manages and controls the release manage process.

Procedures

Intermedia has detailed information security, availability and confidentiality procedures which are designed and categorized from harmonized and applicable requirements of NIST 800-53, ISO 27002 and PCI DSS control families, including but not limited to the following:

Human Resources Hiring and Termination

Documented job descriptions are in place to define employee responsibilities and evaluate job candidates. Candidates are not granted access to facilities and/or systems until a background screening has been completed. Once hired, new employees are required to review the employee handbook and sign off on the terms of the requirements.

Access Authentication and Authorization

Access to Intermedia systems is controlled by user groups and requires a unique user ID and password. Employees are granted access to user groups based on their roles within the organization. Approved personnel have the ability to connect to the Intermedia network remotely through a VPN with multi-factor authentication.

Access Requests and Access Revocation

Access requests for employees, contractors and vendors are initiated by the submission of a standard form. The IT support team disables the user's access upon termination. On a semi-annual basis, a recertification of user access is performed to confirm that user access to systems remains appropriate based on their current role in the organization.

Change Management

Changes to infrastructure, systems, applications, and networks that may impact Intermedia's ability to provide services to customers are logged, tracked, and monitored through a change management system. Any major change resulting in a design or a functionality difference requires notice to impacted customers.

Data

Data as defined for Intermedia’s in-scope systems includes electronic data or information submitted by the customer to Intermedia. Access to information is restricted to authorized personnel and access is granted after receiving proper approval from management. Intermedia has developed an Information Sensitivity Policy to help personnel determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Intermedia without proper authorization.

Intermedia has developed the Acceptable Encryption Standard to provide guidance that limits the use of encryption algorithms. Per the Acceptable Encryption Standard, Intermedia requires the data to be encrypted when confidential information is in transit on a network or is stored on systems or devices located outside the Intermedia network. Tape Backup media is encrypted at the time of creation by policies.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Unite Chat- chat and attachments, directory, voicemails, voice calls, meeting, files, other Personally identifiable data	Customer Unite Application- Desktop, and Mobile	Confidential
Cloud PBX - call statistical information, recordings, end-user callback phone numbers	Customer Cloud PBX portal	Confidential
Hosted Exchange – e-mail messages and corresponding attachment data, folder structure, contacts, calendar, and tasks	Customer Hosted Exchange Portal, E-mail client	Confidential
SecuriSync - customer submitted file content and data	Customer SecuriSync Portal	Confidential
AnyMeeting – customer web meeting data and meeting configurations	Customer AnyMeeting Portal	Confidential

Subservice Organizations

The data center hosting services provided by the third-party data centers were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at the third-party data center providers, alone or in combination with controls at Intermedia, and the types of controls expected to be implemented at the third-party data center providers to meet those criteria.

Control Activity Expected to be Implemented by the Subservice Organizations	Applicable Trust Services Criteria
Third-party data center providers are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 CC6.5

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, processing integrity, confidentiality, and privacy categories are applicable to the Hosted Exchange and Unite systems.