INTERMEDIA
CLOUD COMMUNICATIONS

ROCKY KNOLL TECHNOLOGIES LLC

# Intermedia: Comprehensive Security

**Published** June, 2020

# INTERMEDIA KEEPS YOUR BUSINESS COMMUNICATIONS SECURE

You can feel confident that your private data is safe with Intermedia. Our system utilizes state-of-the-art technologies designed to constantly monitor for, and defend against, malicious intruders.

The Intermedia Security Platform includes these 5 primary security pillars which are constantly evolving in order to respond to, and mitigate, any potential threat. These 5 pillars are regularly examined and reviewed by the Intermedia security team to ensure our customers of a super-secure communications & collaboration experience that can be trusted to protect them and their businesses.

Infrastructure & Network Security

Data Protection & Privacy

Phones/Devices/ App Security

Monitoring & Detection

Security Compliance

# 1 INFRASTRUCTURE & NETWORK SECURITY

Intermedia invests considerable human and capital resources to help ensure high levels of security and protection that give you peace of mind. Infrastructure and Network Security is one of the pillars of our Worry-Free Experience. We understand that if you're to trust us with your communications and data, you need to understand how we'll protect it. Vigilance is essential to keeping your business safe.

### Highly Secure Datacenters

Intermedia's cloud is hosted in geographically dispersed, highly secure and monitored datacenters by certified tier-three providers.

Each of Intermedia's world-class 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 man-trap devices between lobby and datacenter, motion sensors, and controlled ID key-cards. Security guards are stationed at the entrance to each site.

### Infrastructure Protection

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 critical

systems and devices, formal policies for authentication and password controls, and configuration standards for firewalls.

Intermedia has also 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 in the security and confidentiality of systems and data.

We also run multiple Antivirus and intrusion protection systems (IPS) (both host and network) 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.

Antivirus and IPS 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
- Intermedia subscribes to Distributed Denial of Service (DDoS) protection through a leading provider of network security
- Production network is physically and logically separated with highly restricted access and multiple authentication levels
- Operational functions include: monitoring, system hardening, and vulnerability scans

## Employee Security

Intermedia employees, regardless of role, 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.

## Dedicated Security Staff and Monitoring

Intermedia 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, managing intrusion detection systems (both host and network), perimeter defense, service and architecture testing, and source code reviews.

# 2 DATA PROTECTION & PRIVACY

At Intermedia, we're committed to protecting the privacy of your data and making sure you are in complete control of where and how it's used. Your cloud contains extremely valuable and confidential content, including intellectual property, customer data, financial information, and sensitive personal data. You need to have confidence in how it's stored and managed.

### Privacy Policy

Intermedia offers a clearly documented Privacy Policy, which governs our treatment and handling of sensitive data, including personally identifiable information. Intermedia also adheres to the EU-U.S. Privacy Shield Framework set forth by the U.S. Department of Commerce and the European Commission.

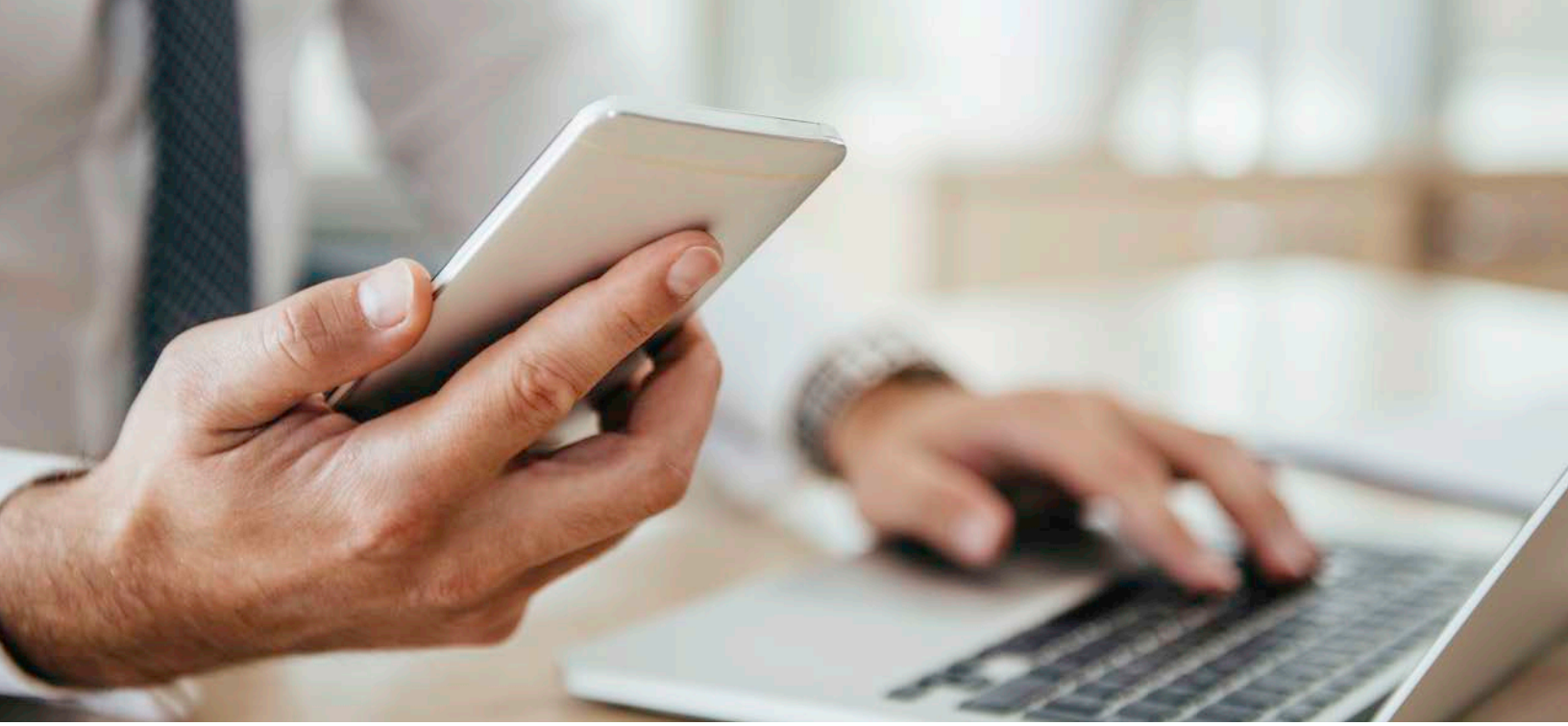
To read Intermedia's Privacy Policy, please visit this link.

### Data Jurisdiction/ Residency

Our Intermedia service uses datacenters located in the Easter and Western United States. In addition, datacenter locations for our service will soon include Canada, the United Kingdom, Germany, Australia, and Japan.

### Data Encryption

Data encryption protects sensitive customer and call data from unauthorized access. In addition, numerous state, federal, and industry regulations regarding customer and patient privacy mandate encryption of data. Intermedia employs encryption, both in-transit (using TLS encryption) and at-rest (using AES 256-bit keys), as an essential component of our "secure-by-design" product architecture to help keep your data private and secure. Data encrypted while at rest includes voicemails, call recordings, meeting recordings/chat/notes, chat and SMS history, chat attachments, and SecuriSync files.



# 3 PHONES / DEVICES / APP SECURITY

Encryption technology is important to keep conversations and data secure from prying eyes. However, encryption only tells part of the story. Intermedia has several technologies that keep intruders from having the ability to access your internal systems and apps.

### Secure Handset Protection

To verify that phones and devices are secure from cyber threats and attacks like eavesdropping, we require strong passwords on all SIP endpoints. Each device is securely provisioned using “HTTPS” with mutual authentication to prevent intrusion.

### Authentication for Apps

The Desktop and Mobile Apps from Intermedia allow users to use their business phone system while working remotely or on the go. These apps can require a login and password and can also be enabled with 2-factor authentication for access.

### Google Chromium Browser Security Platform

The Intermedia Desktop App is built using Google Chromium browser technology. It makes use of the very latest security enhancements available and is updated regularly to keep current with the latest security patches. Chromium’s architecture focuses on preventing attacks from persistent malware, transient keyloggers, and file theft.

# 4 MONITORING & DETECTION

**Automated 24/7 Toll Fraud & Threat Detection**

Intermedia monitors call patterns to international (and high-cost) locations on a constant basis and consistently looks to improve our fraud monitoring systems.

If any customer exceeds the call thresholds for any international areas, Intermedia will disable international calling and send an email notification to the customer informing them that international calling has been disabled based on possible fraudulent activity. To protect the customer, we will not re-enable international calling until the account holder has given Intermedia authorization.

Additionally, Intermedia employs active monitoring to detect and notify customers of suspicious login activity and unrecognized devices on their network.

**Spam Caller Protection**

Every account is enabled with Spam Caller Protection – helping to keep you and your employees free from calls originated by autodialers and known fraudsters. To learn more, see our article about Spam Caller Protection.

# 5 SECURITY COMPLIANCE

### SOC 2

SOC 2 is a technical audit specifically designed for service providers who store customer data in the cloud. Intermedia has a SOC 2 report from an independent auditor that has validated that, in their opinion, Intermedia's controls and processes are effective in minimizing risk and exposure to this data.
Download Intermedia's SOC 3 report here.

### 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 Intermedia to establish and maintain systems designed to ensure that we protect our subscribers' Customer Proprietary Network Information (CPNI).

Each year, Intermedia files an annual certification documenting our compliance with these rules.

### PCI-DSS

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 Intermedia has passed these strict testing procedures, and is compliant with the Standard. This helps ensure that your payment information will not be accessed by unauthorized parties or shared with unscrupulous vendors.

### Privacy Shield and GDPR

Intermedia has extensive experience managing a highly secure infrastructure and complying with complex regulations. As noted above, we currently self-certify compliance with the EU-US Privacy Shield framework (access our Privacy Shield Notice here) and are committed to comply with the EU's General Data Protection Regulation (GDPR) across our services. Intermedia maintains a security environment that meets the requirements of the GDPR, and we offer GDPR-compliant Data Processing Addendums (DPAs) to our partners and customers to help assure them that our processing and handling of their data will meet the GDPR's standards.

Click here for more information about GDPR compliance.

**HIPAA**

The confidentiality and security or "privacy" rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require entities that engage in HIPAA transactions to protect sensitive health information against disclosure to unauthorized parties.

When combined with your strong internal security policies and procedures, the Intermedia service (using the recommended settings shown below) helps to safeguard Protected Health Information (PHI) by adhering to the required administrative, physical, and technical standards outlined in the HIPAA Security Rule.

Intermedia can partner with healthcare organizations to help protect your PHI. If you are subject to HIPAA's requirements, ask your Intermedia Sales Representative about putting in place a Business Associate Agreement (BAA).

## INTERMEDIA HIPAA GUIDANCE

| | HIPAA COMPLIANCE | INTERMEDIA RECOMMENDS |
|---|---|---|
| Calling | ✓ ACTION SUGGESTED | The account can request that TLS encryption be enabled |
| Mobile Softphone | ✓ ACTION SUGGESTED | TLS can be enabled by the user for greater privacy |
| Call Recording | ✓ ACTION SUGGESTED | The administrator may disable call recording notifications for greater security |
| Voicemail to Email | ✓ ACTION SUGGESTED | The administrator may disable Voicemail to Email notifications for greater security |
| Voicemail Transcription | ✓ ACTION SUGGESTED | The administrator may disable Voicemail Transcription notifications for greater security |
| Visual Voicemail | ✓ | Visual Voicemail is only available in the mobile app, and is protected by 2-factor authentication |
| Desktop Softphone | ✓ | Desktop Softphone uses Secure WebRTC encryption for signaling and media |
| SMS | ✓ | SMS information is encrypted at rest. Sent messages are encrypted in transit between Intermedia and its partner networks.* |
| Chat | ✓ | Encrypted at rest and in transit |
| SecuriSync® | ✓ | Encrypted at rest and in transit |
| AnyMeeting® meetings, chat, notes | ✓ | Encrypted at rest and in transit |
| Extend Integrations | NOT APPLICABLE | Integrations with 3rd party applications are not covered under the HIPAA BAA |

## SECURITY

| | HIPAA COMPLIANCE | INTERMEDIA RECOMMENDS |
|---|---|---|
| Business Associate Agreement | ✓ | For covered entities, a Business Associate Agreement (BAA) is required for HIPAA compliance |

**Customer security policies governing usage of the Intermedia desktop or mobile applications should require patient consent prior to sending any Patient Health Information unencrypted and unauthenticated via SMS*



**Questions? Contact RKT today.**
704.594.7292 | info@rockyknolltech.com
rockyknolltech.com/phones

ROCKY KNOLL TECHNOLOGIES LLC