RingCentral Internet Usage and Monitoring Policy

I. Purpose

The purpose of this policy is to define standards for systems that monitor activity within RingCentral's network. These standards are designed to ensure individuals use RingCentral network and devices in a safe and responsible manner.

II. Scope

This policy applies to all RingCentral employees, contractors, vendors and agents with devices (including but not limited to computers, tablets, mobile devices, network capable appliances) connecting to the RingCentral network. This also applies to all end user initiated communications between RingCentral's network and the Internet, including but not limited to web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

III. Policy

A. Roles and Responsibilities

1. Legal
   - ❖ Applying and enforcing internet policy usage during the induction period of new employees to reduce the risk of abuse that will lead to legal liabilities and may hurt the company's reputation.
2. Human Resources
   - ❖ Implement an Employee Internet Management (EIM) solution to achieve a balance between professional and personal employee Internet use in the workplace. HR will accommodate both employee and employer web concerns to take a more educated, proactive role in managing employee Internet use at work.
   - ❖ Managing employees lost productivity due to internet abuse.
3. SecOPS
   - ❖ Monitor all network data flow and respond to known, unknown and advanced threats.
4. IT Administrator
   - ❖ Technically implement all related policies
   - ❖ Respond to escalations by SecOPS in relation to violations and security threats
5. IT Management
6. All Employees and Users on RingCentral's Network
   - ❖ Use network resources for business use only
   - ❖ Not to store credit card information via RingCentral networks.

B. Network Monitoring

RingCentral will carry out automated monitoring of its IT and communications systems through automated tools such as anti-malware software, website filtering and spam filtering. It will also carry out monitoring of its physical premises, for example by using CCTV and badge scans.

C. Access to Web Site Monitoring Reports

The activity and trending reports will be available to SecOPS and IT Teams. The same data can be made available to Management upon HR Approval.

D. Internet Use Filtering System

The Information Technology Department will block access to Internet websites and protocols that are deemed inappropriate for RingCentral's corporate environment. The following protocols and categories of websites should be blocked including but is not limited to:

1. Generally Blacklisted Categories (GBC)
    a) Adult/Sexually Explicit Material
    b) Advertisements & Pop-Ups
    c) Gambling
    d) Hacking
    e) Illegal Drugs
    f) Intimate Apparel and Swimwear
    g) Peer to Peer File Sharing
    h) Personals and Dating
    i) SPAM, Phishing and Fraud
    j) Spyware
    k) Tasteless and Offensive Content
    l) Violence, Intolerance and Hate

2. Customer Data Environment (CDE) Blacklisted Categories (includes GBC)
    a) Social Network Services
    b) Chat and Instant Messaging
    c) Web Based Email

E. Internet Use Filtering Rule Changes (Company-Wide)

The Information Technology Department will periodically review and recommend changes to web and protocol filtering rules. Security, IT and Legal will review these recommendations and decide if any changes are to be made. Changes to

web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

F. Internet Use Filtering Exceptions (Individual)

If a site is mis-categorized, employees may request the site be unblocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and unblock the site if it is mis-categorized. Access to blocked sites will be allowed with permission if appropriate and necessary for business purposes. Access to a site that is blocked and appropriately categorized can be requested by submitting a request to IT. IT will present all approved exception requests to Security, IT, and Legal in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

IV. Policy Compliance

A. Compliance Measurement

The SecOPS Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

B. Exception

Any exception to the policy must be approved by the SecOPS Team in advance.

C. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Please refer to the Employee handbook
https://wiki.ringcentral.com/download/attachments/202576731/US+RC+Handbook.pdf?version=1&modificationDate=1447439026000

V. Monitoring Purpose and Awareness

A. The primary purpose of this monitoring is to protect RingCentral, its employees, customers and business partners, for example:

1. for general network operation and security, including in particular the security of RingCentral's IT systems and assets, and the optimal operation of its network and devices;
2. for proof of business transactions and archiving;
3. for coaching, training and evaluation of employees;
4. for the protection of confidential information and intellectual property;
5. for investigating breaches of internal policies, fraud or other unlawful or wrongful activity, or to respond to a particular personnel or company incident;
6. for business continuity (such as monitoring business-related emails following an employee's departure); and
7. for physical security of its premises.

B. Monitoring activities are likely to be continuous and ongoing. However, they will always be proportionate, for legitimate purposes and as required or permitted by applicable law. Before undertaking any monitoring activities, we will consider your reasonable expectations of privacy and assess whether there are any less invasive options.

C. You should be aware that any message, files, data, document, facsimile, telephone conversations, social media post or instant message communications, or any other types of information transmitted to or from, received or printed from, or created, stored or recorded on our IT and communications systems and assets are presumed to be business-related and may be monitored by us in accordance with applicable law.

D. You must clearly identify private emails and messages by adding the term "private & confidential" in the email or message's subject line, and/or storing those emails/messages/files in a separate folder marked "private & confidential". Where we must access content that is clearly identifiable as being private, we will do so only if there is a particular risk or threat to the company, or person, or we have been legally authorised to do so, for example by a court order.

Definitions and Terms

E. Peer to Peer File Sharing

F. Social Networking Services

G. SPAM
H. Phishing
I. Hacking

VI. Revision History

Date of Change	**Responsible**	**Summary of Change**
January 2016	Carlo Curato	Draft -v1.0
May 2018	Fred Chin	Draft -v2.0