

## RTC Acceptable Use Policy ("AUP")

RTC has published this Acceptable Use Policy ("AUP") as part of our overall effort to provide high-quality, reliable service to our clients; protect the privacy and security of our clients, systems, and networks; encourage responsible use of network resources; and comply with applicable laws. This AUP is an integral part of your Agreement with RTC for the provision of Services set forth on Service Description Exhibit. This AUP describes the types of uses which are contrary to our objectives and which are, therefore, prohibited. To achieve our objectives, RTC may in its sole discretion determine whether a use of our Services is a violation of this Policy. Your services may be suspended or terminated for violation of this AUP in accordance with your services Agreement with RTC. Clients are responsible for keeping informed of the current AUP in effect, including any revisions or updates, and for abiding by the terms of this AUP. Capitalized terms used in this AUP shall have the meaning given in your Agreement.

Client will not be issued a credit for any interruption in service resulting from violations of this AUP. You are solely liable and responsible for your use of the RTC Services.

### Illegal Use

Any use of RTC Services in a manner which is defined or deemed to be statutorily illegal is a direct violation of RTC's AUP. This includes, but is not limited to: death threats, terroristic threats, threats of harm to another individual, multi-level marketing schemes, "Ponzi schemes" or other fraudulent activities, invasion of privacy, credit card fraud, racketeering, defamation, slander, and other common illegal activities.

### Abuse

You may not use RTC's network or services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

- The storage, distribution, fabrication, or use of malware including virus software, root kits, password crackers, adware, keystroke capture programs and other programs normally used in malicious activity; provided, however, programs used in the normal ordinary course of business are deemed acceptable.
- Any activity associated with phishing or systems designed to collect personal information (name, account numbers, user names, passwords, etc.) under false pretense. Splash pages, phishing forms, email distribution, proxy email or any relation to phishing activities will result in immediate removal.
- Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Interference with service to any user of the RTC or other network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- Use of an Internet account or computer without the owner's authorization;
- Collecting or using email addresses, screen names or other identifiers without the consent of the person identified (including, without limitation, phishing, Internet scamming, password robbery, spidering, and harvesting);
- Collecting or using information without the consent of the owner of the information;
- Use of any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting;

- Use of the service to distribute software that covertly gathers information about a user or covertly transmits information about the user;
- Use of the service for distribution of advertisement delivery software unless: (i) the user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software, and (ii) the software is easily removable by use of standard tools for such purpose included on major operating systems; (such as Microsoft's "ad/remove" tool); or
- Any conduct that is likely to result in retaliation against the RTC network or website, or RTC's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack. RTC absolutely prohibits the use of services or network services for the origination or control of denial of service ("DoS") attacks or distributed denial of service ("DDoS") attacks. Any relation to DoS or DDoS type activity is a direct violation of RTC's AUP.

## Server Abuse

Any attempts to undermine or cause harm to a RTC server or subscriber of RTC is strictly prohibited including, but not limited to:

- Logging into a server or account that you are not authorized to access;
- Accessing data or taking any action to obtain services or information not intended for you or your use without the consent of the owner;
- Tampering, hacking, modifying, or otherwise corrupting or breaching security or authentication measures without proper authorization;
- Transmitting material that contains viruses, Trojan horses, worms, time bombs, cancelbots or other computer programming routines or engines with the intent or effect of damaging, destroying, disrupting or otherwise impairing a computer's functionality or the operation of the RTC's systems;
- Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- Interfering with, intercepting or expropriating any system, data or information which you do not have the right to access; and
- Interfering with service to any user, host or network including, without limitation, by means of overloading, "flooding," "mail-bombing," or "crashing" any computer system.

You agree that we may quarantine or delete any data stored on the RTC network if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the network or other clients' data that is stored on the network. You further agree to take corrective action immediately upon notification by RTC or any third part that indicates that the security or integrity of one or more of the computer systems or networks under your control have been compromised. Failure to take immediate action will result in RTC personnel taking steps to mitigate the problem at your expense.

## Export Regulations

You represent and warrant that you are not on the United States Department of Treasury, Office of Foreign Asset Controls list of Specially Designated National and Blocked Persons and are not otherwise a person to whom RTC is legally prohibited to provide the Services. You may not use the Services for the development, design, manufacture, production, stockpiling, or use of nuclear, chemical or biological weapons, weapons of mass destruction, or missiles, in a country listed in Country Groups D: 4 and D: 3, as set forth in Supplement No. 1 to the Part 740 of the United States Export Administration Regulations, or as otherwise prohibited by law, nor may you provide administrative access to the Service to any person (including any natural person or government or

private entity) that is located in or is a national of any country that is embargoed or highly restricted under United States export regulations.

## Bulk Email

You may not use any RTC Service to send Bulk Mail. "Bulk Mail" means email messages of similar content that are sent to more than two hundred and fifty (250) recipients. Attempts to circumvent this restriction by breaking up bulk email over time, using multiple accounts, or other means will be a violation of this restriction. A mail message sent to other users within your domain names hosted on the RTC system is not considered Bulk Mail.

## Mail Requirements

You may not send unsolicited email. Email is unsolicited if you have no pre-existing relationship with the recipient, unless the recipient has published or otherwise provided his or her email address in a manner which implies consent to receive the email. You may not send email of any kind to a person who has indicated that they do not wish to receive it. Any such email shall comply with all laws and regulations, including without limitation, the CAN SPAM Act. In addition, your bulk and commercial email must meet the following requirements:

- Your intended recipients have given you their consent to receive email from you via some affirmative means, such as an opt-in procedure ("Opt-out only" is not acceptable);
- Your procedures for seeking consent include reasonable means to ensure that the person giving consent is the owner of the email address for which consent is given;
- You retain evidence of each recipient's consent in a form that can be promptly produced on request, and you honor recipient's and RTC's requests to produce consent evidence within 72 hours of receipt of the request;
- You have procedures in place that allow a recipient to revoke their consent - such as a link in the body of the email, or instructions to reply with the word "Remove" in the subject line; you honor revocations of consent within 48 hours, and you notify recipients that the revocation of their consent will be implemented in 48 hours;
- You must post an email address for complaints (such as [abuse@yourdomain.com](mailto:abuse@yourdomain.com)) in a conspicuous place on any website associated with the email, you must register that address at abuse.net, and you must promptly respond to messages sent to that address;
- You must have a Privacy Policy posted for each domain associated with the mailing;
- You have the means to track anonymous complaints;
- You may not obscure the source of your email in any manner, such as omitting, forging, or misrepresenting message headers or return addresses. Your email must include the recipients email address in the body of the message or in the "TO" line of the email;
- The subject line of the email must clearly describe the subject matter contained in the email, and the message must include valid contact information; and
- You must not attempt to send any message to an email address if 3 consecutive delivery rejections have occurred and the time between the third rejection and the first rejection is longer than fifteen days.

These policies apply to messages sent using your RTC services, or to messages sent from any network by you or any person on your behalf that directly or indirectly refer the recipient to a site or an email address hosted via your RTC service. In addition, you may not use a third party email service that does not practice similar procedures for all its clients. These requirements apply to distribution lists prepared by third parties to the same extent as if the list were created by you. RTC may test and otherwise monitor your compliance with its requirements. RTC may block the transmission of email that violates these provisions. RTC may, at its discretion, require certain clients to seek advance approval for bulk and commercial email, which approval will not be granted unless the client can

demonstrate that all of the requirements stated above will be met. Complaints from email recipients and third-party abuse agencies (e.g. SpamHaus or Spamcop) shall be deemed proof of the facts stated therein unless you provide compelling evidence to the contrary. RTC shall have the right to terminate your mail service if we receive excessive or repeated complaints from your email recipients, regardless of whether you are in breach of this AUP or are otherwise at fault.

## Unsolicited Communications

You may not use your service to send email or any other communications to a person who has indicated that they do not wish to receive it. If the communication is bulk mail, then you will not be in violation of this section if you comply with the 48 hour removal requirement described above.

## Vulnerability Testing

You may not attempt to probe, scan, penetrate or test the vulnerability of a RTC system, subsystem or network or to attempt to breach security or authentication measures, whether by passive or intrusive techniques, without RTC's express written consent.

## Newsgroup, Chat Forums, Other Networks

You must comply with the rules and conventions for postings to any bulletin board, chat group or other forum in which you participate, such as IRC and USENET groups including their rules for content and commercial postings. These groups usually prohibit the posting of off-topic commercial messages, or mass postings to multiple forums.

You must comply with the rules of any other network you access or participate in using your RTC services.

## Offensive Content

You may not publish, transmit or store on or via RTC's network and equipment any content or links to any content that RTC reasonably believes:

- Constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, or non-consensual sex acts;
- is excessively violent, incites violence, threatens violence, or contains harassing content or hate speech;
- is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
- is defamatory or violates a person's privacy;
- creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with a investigation by law enforcement;
- improperly exposes trade secrets or other confidential or proprietary information of another person;
- is intended to assist others in defeating technical copyright protections;
- infringes on another person's copyright, trade or service mark, patent, or other property right;
- promotes illegal drugs, violates export control laws, relates to illegal gambling, or illegal arms trafficking;
- is otherwise illegal or solicits conduct that is illegal under laws applicable to you or to RTC; or
- is otherwise malicious, fraudulent, or may result in retaliation against RTC by offended viewers or recipients, or
- is intended to harass or threaten.

Content "published or transmitted" via RTC's network or equipment includes Web content, email, bulletin board postings, chat, tweets, and any other type of posting or transmission that relies on the Internet.

## Live Events

You may not use your RTC services to stream live sex acts of any kind, even if the content would otherwise comply with the AUP. RTC may prohibit you from streaming other live events where there is a special risk, in RTC's reasonable discretion, that the event may violate the Offensive Content section above.

## Copyrighted Material

You may not use RTC's network or services to download, publish, distribute, or otherwise copy or use in any manner any text, music, software, art, image, or other work protected by copyright law unless:

- you have been expressly authorized by the owner of the copyright for the work to copy the work in that manner; or
- you are otherwise permitted by established copyright law to copy the work in that manner.

It is RTC's policy to terminate in appropriate circumstances the services of clients who are repeat infringers.

## Shared Systems

You may not use any shared system provided by RTC in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example, we may prohibit the automated or scripted use of RTC Mail Services if it has a negative impact on the mail system, or we may require you to repair coding abnormalities in your Cloud-hosted code if it unnecessarily conflicts with other Cloud clients' use of the Cloud. You agree that we may quarantine or delete any data stored on a shared system if the data is infected with a virus, or is otherwise corrupted, and has the potential to infect or corrupt the system or other clients' data that is stored on the same system.

## Other

- You must have valid and current information on file with your domain name registrar for any domain hosted on the RTC network.
- You must request authorization to store, process, or transmit cardholder data or sensitive authentication data through any RTC system components that are included in or connected to your cardholder data environment as defined by the Payment Card Industry standards. RTC reserves the right to accept or deny requests at its sole discretion and may suspend or terminate services for violation of this AUP in accordance with your services Agreement with RTC.
- You must request authorization to connect a wireless access point in your designated space i.e. rack/cage in any of the RTC Data Centers. Wireless access points may only be turned on/active while a client contact is physically onsite at one of the data centers. If a client wireless access point is found to be active within an RTC data center and a client contact is not physically present, RTC will disconnect the device immediately. RTC reserves the right to accept or deny wireless access point requests at its sole discretion and may terminate wireless access point connects for violation of this AUP in accordance with your services Agreement with RTC.

- If you are a controller or processor of personal data of natural persons throughout the European Union, you must request authorization to store, process, or transmit that data through any RTC system and/or components that are included in or connected to your client environment. RTC reserves the right to accept or deny requests at its sole discretion and may suspend or terminate services for violation of this AUP in accordance with your services Agreement with RTC.
- You play a crucial role in achieving the overall objectives mentioned in this policy. You are strongly encouraged to develop and implement information technology best practice controls within your own environment as described in industry-recognized control frameworks published by standard setting organizations such as but not limited to NIST, ISACA, and/or ISO.
- You may only use IP addresses assigned to you by RTC in connection with your RTC services.
- You agree that if the RTC IP numbers assigned to your account are listed on an abuse database, you will be in violation of this AUP, and RTC may take reasonable action to protect its IP numbers, including suspension and/or termination of your service, regardless of whether the IP numbers were listed as a result of your actions.
- You agree that if you register a DNS record or zone on RTC managed or operated DNS servers or services for a domain of which you are not the registrant or administrative contact according to the registrars WHOIS system, that, upon request from the registrant or administrative contact according to the registrars WHOIS system, RTC may modify, transfer, or delete such records or zones.
- We do not allow game servers (dedicated game server programs) of any kind.
- You may not obscure the source of your email in any manner, including by intentionally omitting, forging, or misrepresenting messages headers or return addresses.
- RTC may terminate your Services if your email address or related IP number(s) is/are blacklisted by any third-party, or RTC is retaliated against as a result of your use of the mail system, regardless of whether you are in breach of this AUP or are otherwise at fault.
- The use of dedicated services to send, receive, forward, or post UseNet unsolicited email or posts is a direct violation of RTC's AUP. This includes UseNet services located within the RTC network or unrelated third party networks.
- You agree to maintain applicable and up-to-date software/hardware licenses in accordance with the license agreements as put forth by the software manufacturer for all client-owned infrastructure residing on RTC managed or operated property. RTC may in its sole discretion determine through any means necessary whether a use of our Services is a violation of this Policy and/or manufacturer software licensing agreements. Your services may be suspended or terminated for violation of this AUP in accordance with your services Agreement with RTC.

## Disclosure To Law Enforcement

Occasionally, RTC is required by law to submit client information to law enforcement officials when presented with a valid subpoena or order from a court or governmental entity. Information requested is disclosed as directed pursuant to the subpoena or order. RTC utilizes great care in keeping client information safe and private and will only release information described in the subpoena order. RTC will notify client of the information request to the extent permitted by the subpoena or order

## SLA

No credit will be available under a RTC service level guaranty or agreement for interruptions of service resulting from AUP violations.

## Third Party Software Policy

This document governs the use of third party products and software, which may include associated media, printed materials, and “online” or electronic documentation (individually and collectively, “Third Party Products”) (i) provided by RTC as part of a Service, (ii) deployed by You in the Provider’s affiliate Data Technology Center, and/or (iii) rented by You through RTC as part of a SPLA or similar program. By purchasing, downloading or deploying any of the Third Party Products, you agree to be bound by the applicable terms for those Third Party Product(s). If you do not agree to be bound by any of the applicable terms for the Third Party Products, then you must not use those Third Party Products. RTC reserves the right to modify this document from time to time. You agree that you will be bound by the most recent version of the Third Party Terms at any point in time.

### I. General Terms of Use Applicable to all Third Party Products

1. **END USER LICENSES.** By installing and using the Third Party Products you agree to comply with the terms and conditions of all end user license agreements or terms of use accompanying any software or plug-ins to such Third Party Products distributed or used in connection with RTC Services, as these agreements may be amended from time to time. All such agreements are incorporated in this Policy by reference.
2. **PRICING AND SERVICES.** Subject to applicable law, and notwithstanding anything to the contrary in the MSA, RTC shall have the right to change the Third Party Products and rates or charges, at any time with or without notice. Features or offerings contained in the Licensed Products, including but not limited to, functionality, hours of availability, and customer equipment requirements may be changed or modified at any time with or without notice. If we do give you notice, it may be provided via email to the Authorizing Officer on your account, on your monthly bill, as a bill insert or other communication permitted under applicable law.
3. **END USER RESPONSIBILITY.** It is your responsibility to track all licenses for all the Third Party Products used by you. You will be responsible for payment for all Third Party Products deployed by you. You will be responsible for any and all fees related to your over deployment of the Third Party Products including any interest, penalties, and third-party audit costs assessed against RTC by a provider of Third Party Products.

## Refund Policy

RTC does not issue payment refunds. Service Level Credits in favor of Client shall be counted against the Service Fees for the applicable month