

Acceptable Use Policy

I. Introduction

24/7 Mid-Atlantic Network, LLC, on behalf of itself and its affiliates (collectively the “Company”), has formulated this Acceptable Use Policy ("AUP") in an effort to promote responsible use of our network, systems, services, web site, and products (“Products”) by our customers and other users (collectively, "Users") from fraud, abuse of resources and irresponsible or illegal activities. By using Company Products, Users consent to be bound by the terms of this AUP as may be modified from time to time.

A. Use of Services

Company makes no guarantee regarding, and assumes no liability for, the security and integrity of content, data or information Users transmit, upload or download via the Products or over the Internet, or for any mistakes, defamation, slander, libel, omissions, falsehoods, obscenity, pornography, or profanity that a User may encounter. Company is only the provider of the facilities and/or services, and shall not be liable for any statements, representations, or content provided by or encountered by Users in any online source. Company does not undertake to monitor, exercise control over, or accept responsibility for the content of information passing through its network. However, Company may monitor content of any such materials as necessary to comply with applicable laws, regulations or other governmental or judicial requests or to protect the Company, its network and/or Users.

User understands and acknowledges that in some instances, the Products may be used to link into other networks worldwide. User agrees to conform to the acceptable use policies of these networks and to conform to the Internet protocols and standards. Any application that overloads Company’s network by whatever means is not permitted. Users who violate systems or network security may incur criminal or civil liability. All persons and organizations, including Users, who transmit information over or who publish information that is made accessible through Company Products are responsible for the content of the information and for complying with all applicable law.

Company Products may only be used for lawful and appropriate purposes. Company Products may not be used in connection with any criminal, civil or administrative violation of any applicable local, state, provincial, federal, national or international law, treaty, court order, ordinance, regulation or administrative rule. Company reserves the right to cooperate with legal authorities in the investigation of suspected criminal or civil violations.

B. Customer Responsibilities

Each customer (including commercial customers, carriers and resellers) is responsible for the activities of its own customers or end-users and, by accepting service from Company agrees to inform its customers and/or end-users of this AUP. By using the Products, Users agree to indemnify, defend and hold harmless, Company, its officers, directors, employees, agents,

licensors, and suppliers from and against all losses, expenses, damages, and costs, including reasonable attorney's fees, resulting from User's violation of this AUP.

Users remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the Products. User recognizes and agrees that Company has no responsibility for any material created on Company network or accessible using the Products, including content provided on third-party websites or networks, even if those websites or networks are accessed through the Products. Users are responsible for taking prompt corrective action to remedy any violation of this AUP and to help prevent similar future violations.

II. Prohibited Conduct

Users may not transmit, retransmit, redirect, or store material in violation of Federal or state laws or regulations, industry or community standards, including, but not limited to, obscenity, indecency, defamatory or material infringing trademarks or copyrights. Users may not abuse or fraudulently use Company Products. The following illustrate some, but not all, uses that are prohibited under this AUP:

A. Security of System and Network

Users are responsible for ensuring and maintaining security of their systems and the machines that connect to and use IP Service(s), including implementation of necessary patches and operating system updates. Violations of any security protocol and/or measure and or device for the system or network are prohibited, and may result in criminal and civil liability. Company reserves the right to investigate incidents involving such violations and may involve and will cooperate with law enforcement if a criminal violation is suspected. Without limiting the generality of the foregoing, the following are examples of such security violations:

- **Unauthorized Access:** Unauthorized access includes the illegal or unauthorized access to other computers, accounts, or networks; using Company Products not included in customer's contract; using the services in a manner that encumbers disk space, processors or other system resources beyond amounts allowed by the type of product; unauthorized monitoring of data or traffic on any network or system without express authorization of the owner of the system or network and/or interfering with a service; hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access or control device, software or data without express authorization of the owner of the system or network.
- **Unlawful Acts:** Use of Company Products to violate the law or in aid of any unlawful act, including uses which constitute an illegal threat or violates export control laws.
- **Denial of Service:** Engaging in activity that may or is intended to interfere with the service of another user, host or network on the Internet.
- **Misleading Messages:** Impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.); forging or misrepresenting a message header

of an electronic transmission; soliciting mail for any other address other than that User, except with full consent of the owner of the referred address.

- Distribution of Harmful Messages/Viruses: Distribution of software, programs or messages that may cause damage or annoyance to persons, data, and/or computer system (such as viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software) or any program, file, script, command or transmission of any message or content of any kind, designed to hi-jack or interfere with the access to or use of the Products or any communication. Hosts not timely secured or removed by Users may be blocked by Company from accessing the network.
- Network Sabotage: Use of Company Products in a manner that interferes with others' use of the Internet or Company's network. distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations).

B. Inappropriate Content

Users may not use Company Products to transmit illegal or inappropriate content such as:

- Spam/E-mail/Usenet Abuse: Messages sent in violation of the CAN-SPAM Act of 2003, or any other applicable law regulating e-mail services, constitutes a violation of this AUP. The transmitting of unsolicited email to multiple recipients, sending large amounts of email repeatedly that annoys, harasses or threatens another person or entity or sending unsolicited electronic messages directed primarily at the advertising or promotion of products or services, petitions for signatures, requests for charitable donations, or sending any chain mail related materials.
- Child Pornography: It is illegal under federal child exploitation statutes to possess, produce, receive, transport or distribute by any means, including computer, visual depictions of "sexual intercourse" and/or "sexually explicit conduct" involving persons under the age of 18. Company Products shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Users must comply with all applicable laws pertaining to the protection of minors
- Inappropriate Content: Using the services to transmit, distribute, redirect, or store material that, as reasonably determined by Company to be inappropriate, obscene, defamatory, libelous, threatening, abusive, malicious, indecent, libelous, treasonous, excessively violent hateful or which contains or incites violence.
- Threatening Material or Content: Company Products shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others.
- Violation of Intellectual Property Rights: Company Products shall not be used to publish, submit/receive upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of the Company or any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret,

trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

- Fraudulent Activities: Fraudulent activities includes, but is not limited to, intentional misrepresentations or misleading statements, writings or activities made with the intent that the person receiving it will act upon it; obtaining services with the intent to avoid payment; hosting of phishing websites and pyramid schemes.
- Non-email Based Spamming: Posting of messages to newsgroups/blogs/services that are irrelevant, blanket posting of messages to multiple newsgroups/blogs/services, and the posting of annoying, harassing and/or threatening messages. Violation of any rules, policies or charters posted online by any search engine, subscription web service, chat area, bulletin board, webpage, or any other service accessed through Company's Products or network is prohibited.
- Facilitating a Violation of this AUP: Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to allow a user to violate this AUP, including, but is not limited to, the facilitation of the means to spam, initiation of ping, flooding, mail bombing, denial of service attacks, and piracy of software.

III. Violations and Enforcement

User's failure to observe the guidelines set forth in this AUP may result in Company taking actions which range from a warning to a suspension or termination of User's Products. When feasible, Company may provide User with a notice of an AUP violation via e-mail or otherwise allowing the User to promptly correct such violation. Company reserves the right, however, to act immediately and without notice to suspend or terminate affected Product(s) in response to a court order or government notice that certain conduct must be stopped or when Company determines, that the conduct may: (1) expose Company to sanctions, prosecution, civil action or any other liability, (2) cause harm to or interfere with the integrity or normal operations of Company or Company's network or networks with which Company, (3) interfere with another User of the Company's Products or the Internet (4) violate any applicable law, rule or regulation, or (5) otherwise present an imminent risk of harm to Company, other Users or the public. Indirect or attempted violations of this AUP, and any actual attempted violations by a third party on behalf of a User or Company Customer shall be considered violations of this AUP by such User or customer.

Company shall not be liable for damages of any nature suffered by any User or any third party resulting in whole or in part from Company exercising its rights under this AUP. Company does not assume liability for others' violations of this AUP or failures to terminate those violations. Company reserves the right to assess time and materials charges to resolve customer issues that are not resolved by the customer in a timely manner.

IV. Other Provisions

A. Contact Information

To report a violation of this AUP or an abuse of Company's Products, please contact us at:

If you believe that your work has been copied and posted, stored or transmitted using the Products in a way that constitutes copyright infringement, please submit a notification pursuant to the Digital Millennium Copyright Act ("DMCA") and directed to the designated agent listed below:

Crown Castle
ATTN: Legal Department
1500 Corporate Drive
Canonsburg, PA 15317
Email: privacy@crowncastle.com

B. Modification

Company reserves the right to modify this AUP in its sole discretion, at any time. Modifications will be effective upon posting. Any use of Company Products after such modification shall constitute acceptance of the modifications in question.

Technology changes rapidly, and any activity not specifically prohibited herein but determined by Company in its sole discretion, to be harmful to other customers or the general operations of the system or network may be halted by Company. In no event shall Company be liable for failing to halt any activity, whether or not specifically proscribed hereunder.

C. Applicable Law

This AUP agreement shall be governed by and construed in accordance with the laws of the State of Maryland without regard to its conflicts of law principles. If any provision of this AUP shall be found to be unlawful, void, or for any reason unenforceable, then the remainder of this agreement, or the application of such provision to persons or circumstances other than those as to which it is held invalid, shall not be affected thereby.